



# Sun Secure Global Desktop 4.5 Installation Guide

---

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 820-6688-10  
April 2009, Revision 01

Submit comments about this document by clicking the Feedback[+] link at: <http://docs.sun.com>

Copyright © Copyright 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Solaris, OpenSolaris, Java, JavaServer Pages, JSP, JVM, and JavaScript are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Adobe is the registered trademark of Adobe Systems, Incorporated.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux États - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Solaris, OpenSolaris, Java, JavaServer Pages, JSP, JVM, and JavaScript sont des marques déposées ou enregistrées de Sun Microsystems, Inc. ou ses filiales aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Adobe est une marque enregistrée de Adobe Systems, Incorporated.

Intel est une marque déposée ou enregistrée de Intel Corporation ou ses filiales aux États-Unis et dans d'autres pays.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des États-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Please  
Recycle



Adobe PostScript

# Contents

---

## **Preface   vii**

### **1.   Preparing to Install   1**

Hardware Requirements   1

Supported Installation Platforms   2

    Installing on Solaris 10 OS Trusted Extensions   3

    Operating System Modifications   3

        Localized Messages During Installation on Linux Platforms   3

        5250 and 3270 Applications   3

        SUSE Linux Enterprise Server 10   3

        Solaris 10 OS   3

        Red Hat Enterprise Linux 5   4

Network Requirements   4

Clock Synchronization   5

SGD Web Server   5

Required Users and Privileges   6

Supported Client Platforms   7

Supported Installation Platforms for the SGD Enhancement Module   8

Application Connection Methods   9

Release Notes   10

## **2. Installing SGD 11**

Performing the Installation 11

▼ How To Install SGD 12

Installing the SGD Enhancement Module for Microsoft Windows 14

▼ How to Install the SGD Enhancement Module for Microsoft Windows 14

Installing the SGD Enhancement Module for UNIX and Linux Platforms 15

▼ How To Install the SGD Enhancement Module on Solaris Platforms 16

▼ How To Install the SGD Enhancement Module on Linux Platforms 17

Troubleshooting Installing the UNIX Audio Module on Linux Platforms 18

Installing the SGD Client Manually 18

▼ How to Install the SGD Client Manually on Microsoft Windows  
Platforms 18

▼ How to Install the SGD Client Manually on Solaris OS and Linux  
Platforms 19

Logging in Using the SGD Client 20

## **3. Upgrading SGD 21**

Before You Upgrade 21

Organizational Changes for Versions 4.40 and Later 21

Upgrades and Early Access Program Software 22

Conditions for Upgrading 22

Before You Upgrade on Solaris OS Platforms 22

Upgrades and Your Existing Configuration 23

Performing the Upgrade 24

Upgrading Evaluation Versions of SGD 24

▼ How to Upgrade a Fully Licensed Single-Server Array 24

▼ How to Upgrade a Fully Licensed Multiple-Server Array 25

Upgrading a Customized SGD Installation 26

Upgrading Customized SGD Web Server Files 26

Upgrading Customized SGD Server Files 26

## Upgrading Other SGD Components 28

- ▼ How to Upgrade the SGD Enhancement Module for Microsoft Windows 28
- ▼ How to Upgrade the SGD Enhancement Module for UNIX® and Linux Platforms 28
- ▼ How to Upgrade the SGD Client Automatically 28
- ▼ How to Upgrade the SGD Client Manually 29

## 4. Getting Started With SGD 31

### Logging In to SGD 31

- ▼ How to Log In to SGD 31

### Using the Webtop 34

#### Running Applications 34

#### Changing Your Settings 36

#### Logging Out 37

### SGD Administration Tools 37

#### The Administration Console 37

##### Starting the Administration Console 37

##### Using the Administration Console 38

#### The `tarantella` Command 41

### Creating Users 42

#### Creating User Profiles and SGD Administrators 43

- ▼ How to Create a User Profile 44
- ▼ How to Add an SGD Administrator 46

### Adding Applications to Webtops 49

#### Creating and Assigning an Application Object 50

- ▼ How to Create an Application Server Object 51
- ▼ How to Create an Application Object 53
- ▼ How to Assign an Application Object 57

### Managing SGD 62

Arrays	64
Monitoring Users	65
User Sessions	65
Application Sessions	65
▼ How to Shadow a User's Application Session	66
Controlling SGD	67
Controlling the SGD Enhancement Module	67
Controlling the SGD Enhancement Module for Microsoft Windows	68
Controlling the SGD Enhancement Module for UNIX and Linux Platforms	68
SGD Network Architecture	69
Client Devices	69
SGD Servers	70
Application Servers	70
Next Steps	70
What You Need to Tell Users	71
Where to Get More Help	71

## 5. Removing SGD 73

Removing SGD	73
▼ How to Remove SGD	73
▼ How to Remove the SGD Enhancement Module for Microsoft Windows	73
▼ How to Remove the SGD Enhancement Module for UNIX® and Linux Platforms	74
▼ How to Remove the SGD Client on Microsoft Windows Platforms (Manual Installation)	74
▼ How to Remove the SGD Client on Microsoft Windows Platforms (Automatic Installation)	75
▼ How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms	75

# Preface

---

The *Sun Secure Global Desktop 4.5 Installation Guide* provides instructions for installing, upgrading, and removing Sun Secure Global Desktop Software (SGD). It also provides instructions on how to get started using the software.

---

## How This Book Is Organized

[Chapter 1](#) describes the things you must know and do before you install SGD.

[Chapter 2](#) describes how to install SGD.

[Chapter 3](#) describes the requirements and procedures for upgrading from a previous version of SGD.

[Chapter 4](#) describes how to log in to SGD and get started using the software.

[Chapter 5](#) describes how you remove SGD.

---

## Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, which is at  
(<http://docs.sun.com>)

This document does, however, contain information about specific SGD commands.

---

## Shell Prompts

Shell	Prompt
C shell	<i>machine-name%</i>
C shell superuser	<i>machine-name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

---

## Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
<b>AaBbCc123</b>	What you type, when contrasted with on-screen computer output	% <b>su</b> Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. To delete a file, type <b>rm</b> <i>filename</i> .

---

**Note** – Characters display differently depending on browser settings. If characters do not display correctly, change the character encoding in your browser to Unicode UTF-8.

---

---

## Related Documentation

The following table lists the documentation for this product. The online documentation is available at:

(<http://docs.sun.com/app/docs/coll/1706.4>)

Application	Title	Part Number	Format	Location
Release Notes	<i>Sun Secure Global Desktop 4.5 Release Notes</i>	820-6687-10	HTML	Online
			PDF	Software DVD and online
Administration	<i>Sun Secure Global Desktop 4.5 Administration Guide</i>	820-6689-10	HTML	Online
			PDF	
User	<i>Sun Secure Global Desktop 4.5 User Guide</i>	820-6690-10	HTML	Online
			PDF	
Administration	<i>Sun Secure Global Desktop 4.5 Gateway Administration Guide</i>	820-6691-10	HTML	Online
			PDF	

---

## Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

---

## Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

[docfeedback@sun.com](mailto:docfeedback@sun.com)

Please include the following document title and part number in the subject line of your email:

*Sun Secure Global Desktop 4.5 Installation Guide*, part number 820-6688-10.

# Preparing to Install

---

This chapter describes the things you must know and do before you install Sun Secure Global Desktop (SGD).

Topics in this chapter include:

- “Hardware Requirements” on page 1
- “Supported Installation Platforms” on page 2
- “Network Requirements” on page 4
- “Clock Synchronization” on page 5
- “SGD Web Server” on page 5
- “Required Users and Privileges” on page 6
- “Supported Client Platforms” on page 7
- “Supported Installation Platforms for the SGD Enhancement Module” on page 8
- “Application Connection Methods” on page 9
- “Release Notes” on page 10

---

## Hardware Requirements

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact a Sun Secure Global Desktop Software sales office (<http://www.sun.com/contact>).

The requirements for a server hosting SGD can be calculated based on the *total* of the following:

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD on the host and runs applications

The following are the requirements for installing and running SGD:

- 1.5 gigabytes of free disk space, plus another 300 megabytes at install time
- 1 gigabyte of random-access memory (RAM)
- 1 gigahertz processor
- Network interface card (NIC)

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 20 megabytes for each user
- On SPARC® technology platforms (SPARC platforms), 15 megahertz for each user
- On x86 platforms, 20 megahertz for each user



---

**Caution** – The actual central processing unit (CPU) and memory requirements can vary significantly, depending on the applications used.

---

## Supported Installation Platforms

The following table lists the supported installation platforms for SGD. The operating systems can be run on physical or virtual environments, provided that the minimum hardware requirements are met and that the virtualization platforms provide complete support for the operating system.

Operating System	Supported Versions
Solaris™ Operating System (Solaris OS) on SPARC platforms	10, 10 Trusted Extensions
Solaris OS on x86 platforms	10, 10 Trusted Extensions
OpenSolaris™ on x86 platforms	2008.11 or later
Red Hat Enterprise Linux (Intel® x86 32-bit and Intel x86 64-bit)	5
SUSE Linux Enterprise Server (Intel x86 32-bit and Intel x86 64-bit)	10

Installation in zones is supported for Solaris 10 OS.

# Installing on Solaris 10 OS Trusted Extensions

When you install SGD on Solaris 10 OS Trusted Extensions platforms, you must install SGD in a labelled zone. Do not install SGD in the global zone.

By default, SGD is installed in the `/opt/tarantella` directory. As the `/opt` directory is read only on Solaris 10 OS Trusted Extensions platforms, you must select another location to install SGD. On Solaris OS platforms, the installation program asks you for the installation directory when you install the software.

## Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

## Localized Messages During Installation on Linux Platforms

When you install SGD on Linux platforms, localized messages in the supported languages can only be displayed if the `gettext` package is installed. If the `gettext` package is not installed, English is used during the installation.

## 5250 and 3270 Applications

The `libXm.so.3` library is required to support 5250 and 3270 applications. This library is available in the OpenMotif 2.2 package.

## SUSE Linux Enterprise Server 10

SGD fails to install if the `libgdbm.so.2` and `libexpat.so.0` libraries are not available on the host. SUSE Linux Enterprise Server 10 contains version 3 and version 1 of these libraries by default. Obtain and install the required version of these libraries before installing SGD.

## Solaris 10 OS

You must install at least the End User Solaris OS distribution to get the libraries required by SGD. If you do not, SGD does not install.

# Red Hat Enterprise Linux 5

The default `/etc/hosts` file for Red Hat Enterprise Linux 5 contains a single entry, which incorrectly maps the host name of the SGD host to the local loopback address, `127.0.0.1`.

Edit the `/etc/hosts` file to remove this mapping, and add a new entry that maps the name of the SGD host to the network Internet Protocol (IP) address of the SGD host. The SGD host name must not be mapped to the local loopback IP address.

---

## Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- Hosts must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- When you install SGD, you are asked for the DNS name to use for the SGD server. The DNS name must meet the following requirements:
  - In a network containing a firewall, use the DNS name that the SGD host is known as *inside* the firewall.
  - Always use fully-qualified DNS names for the SGD host. For example, `boston.indigo-insurance.com`.

The *Sun Secure Global Desktop 4.5 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls. The following information lists the common ports used.

Client devices must be able to make Transmission Control Protocol/Internet Protocol (TCP/IP) connections to SGD on the following TCP ports:

- **80** - For Hypertext Transfer Protocol (HTTP) connections between client devices and the SGD web server. The port number can vary depending on the port selected on installation.
- **443** - For HTTP over Secure Sockets Layer (HTTPS) connections between client devices and the SGD web server.
- **3144** - For standard (unencrypted) connections between the SGD Client and the SGD server.
- **5307** - For secure connections between the SGD Client and the SGD server. Secure connections use Secure Sockets Layer (SSL).

---

**Note** – The initial connection between an SGD Client and an SGD server is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open to connect to SGD. You can configure SGD to always use secure connections.

---

To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine the TCP ports that must be open, for example:

- **22** – For X and character applications using Secure Shell (SSH)
- **23** – For Windows, X, and character applications using Telnet
- **3389** – For Windows applications using Windows Terminal Services
- **6010** and above – For X applications

---

## Clock Synchronization

In SGD, an array is a collection of SGD servers that share configuration information. As the SGD servers in an array share information about user sessions and application sessions, it is important to synchronize the clocks on the SGD hosts. Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

---

## SGD Web Server

When you install SGD, you install the SGD web server. The SGD web server consists of an Apache web server and a Tomcat JavaServer Pages™ (JSP™) technology container preconfigured for use with SGD.

When you install SGD, the SGD installation program asks you for the TCP port that the SGD web server listens on for HTTP connections. This is usually TCP port 80. If another process is listening on that port, the installation program asks you to choose another port.

The minimum Java™ Virtual Machine (JVM™) software heap size for the Tomcat JSP technology container is 256 megabytes.

---

# Required Users and Privileges

To install SGD, you must have superuser (root) privileges.

The system must have `ttaserv` and `ttasys` users and a `ttaserv` group before you can install SGD.

The `ttasys` user owns all the files and processes used by the SGD server. The `ttaserv` user owns all the files and processes used by the SGD web server.

The SGD server does not require superuser (root) privileges to run. The SGD server starts as the root user and then downgrades to the `ttasys` user.

If you try to install the software without these users and group in place, the installation program stops without making any changes to the system and displays a message telling you what you need to do. The message includes details of an install script that you can run to create the required users and group.

If you need to create the required users and group manually, the following are the requirements:

- The user names must be `ttaserv` and `ttasys`.
- The group name must be `ttaserv`.
- You can use any user identification number (UID) or group ID (GID) you want. The UID and GID can be different.
- Both users must have `ttaserv` as their primary group.
- Both users must have a valid shell, for example `/bin/sh`.
- Both users must have a *writable* home directory.
- For security, lock these accounts, for example with the `passwd -l` command.

One way to create these users is with the `useradd` and `groupadd` commands, for example:

```
# groupadd ttaserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasys -m ttasys
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv -m ttaserv
# passwd -l ttasys
# passwd -l ttaserv
```

To check whether the `ttasys` and `ttaserv` user accounts are correctly set up on your system, use the following commands.

```
# su ttasys -c "/usr/bin/id -a"
# su ttaserv -c "/usr/bin/id -a"
```

If your system is set up correctly, the command output should be similar to the following examples.

```
uid=1002(ttaserv) gid=1000(ttaserv) groups=1000(ttaserv)
uid=1003(ttasys) gid=1000(ttaserv) groups=1000(ttaserv)
```

# Supported Client Platforms

The following table lists the supported client platforms for the SGD Client. Also included are the supported browsers, and the supported desktop menu systems when the SGD Client is operating in Integrated mode.

Supported Client Platform	Supported Browsers	Integrated Mode Support
Microsoft Windows Vista (Intel x86 32-bit)	Internet Explorer 6 Internet Explorer 7 Mozilla Firefox 2 Mozilla Firefox 3	Microsoft Windows Start Menu
Microsoft Windows XP Professional (Intel x86 32-bit)	Internet Explorer 6 Internet Explorer 7 Mozilla Firefox 2 Mozilla Firefox 3	Microsoft Windows Start Menu
OpenSolaris version 2008.11 or later on x86 platforms	Mozilla Firefox 2 Mozilla Firefox 3	Sun Java™ Desktop System (Java Desktop System) Launch Menu
Solaris 10 OS on SPARC platforms	Mozilla Firefox 2 Mozilla Firefox 3	Java Desktop System Launch Menu
Solaris 10 OS on x86 platforms	Mozilla Firefox 2 Mozilla Firefox 3	Java Desktop System Launch Menu
Solaris 10 OS Trusted Extensions on x86 platforms	Mozilla Firefox 2 Mozilla Firefox 3	Not supported
Mac OS X 10.5	Safari 2 Mozilla Firefox 2 Mozilla Firefox 3	Not supported
Red Hat Enterprise Linux 5 Desktop (Intel x86 32-bit)	Mozilla Firefox 2 Mozilla Firefox 3	Gnome or KDE Start Menu
Ubuntu 8 (Intel x86 32-bit)	Mozilla Firefox 2 Mozilla Firefox 3	Gnome Start Menu

For OpenSolaris operating system client platforms, the `libXm.so.4` library must be present in the `/usr/lib` directory on the client. A copy of this library is included in the `/opt/tarantella/lib` directory on the SGD host.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript™ programming language enabled.

To support the following functionality, browsers must have Java™ technology enabled:

- Downloading and installing the SGD Client automatically
- Determining proxy server settings from the user's default browser

If Java technology is not available, the SGD Client can be downloaded and installed manually.

The following are the supported plug-ins for Java technology:

- Java™ Plugin tool version 1.6.0
- Java Plugin tool version 1.5.0

---

**Note** – Java Plugin tool version 1.6.0 is the *only* supported plug-in for Microsoft Windows Vista platforms.

---

When users start more than one user session using the same client device and browser, the user sessions join rather than the new session ending the existing session. For user sessions to join in this way, the browser must be configured to allow permanent cookies. If permanent cookies are not allowed, user sessions always end and this might cause application windows to disappear.

For best results, client devices must be configured for at least 256 colors.

---

## Supported Installation Platforms for the SGD Enhancement Module

The SGD Enhancement Module is a software component that can be installed on an application server to provide the following additional functionality when using applications displayed through SGD:

- Advanced load balancing
- Client drive mapping (CDM)
- Seamless windows (Windows platforms only)

- Audio (UNIX® or Linux platforms only)

The following table lists the supported installation platforms for the SGD Enhancement Module. The operating systems can be run on physical or virtual environments, provided that the virtualization platforms provide complete support for the operating system.

Operating System	Supported Versions
Microsoft Windows (Intel x86 32-bit and Intel x86 64-bit)	Windows Server 2008 Windows Server 2003 Microsoft Windows XP Professional Microsoft Windows Vista Ultimate Microsoft Windows Vista Business
Solaris OS on SPARC platforms	8, 9, 10, 10 Trusted Extensions
Solaris OS on x86 platforms	10, 10 Trusted Extensions
OpenSolaris on x86 platforms	2008.11 or later
Red Hat Enterprise Linux (Intel x86 32-bit)	5

Note the following limitations:

- On Microsoft Windows XP Professional and Microsoft Windows Vista platforms, only CDM is supported. Seamless windows and advanced load balancing are not supported. Only full Windows desktop sessions are supported. Running individual Windows applications is not supported for these platforms.
- On Solaris 10 OS Trusted Extensions platforms, audio and CDM are not supported.

Application servers that are not supported platforms for the SGD Enhancement Module can be used with SGD to access a supported application type using any of the supported protocols.

# Application Connection Methods

To run applications, SGD must be able to connect to the application server that hosts the application. Typically this is done using either Telnet or SSH. Enable one of these services before installing SGD. SSH is the best for security.

If you are using SSH, you must enable X11 forwarding. You can do this either in your SSH configuration or by configuring the application in SGD. The *Sun Secure Global Desktop 4.5 Administration Guide* has details on using SSH with SGD.

---

# Release Notes

Before installing SGD, read the *Sun Secure Global Desktop 4.5 Release Notes*. The release notes contain important information about this version of SGD, including the known issues and bugs with installation.

## Installing SGD

---

This chapter describes how to install Sun Secure Global Desktop (SGD).

If you are upgrading, read the upgrade instructions in [Chapter 3](#) *before* installing the software.

SGD contains several installable components:

- The component installed on *hosts* provides the main functionality of SGD.
- The component installed on *application servers*, called an SGD Enhancement Module, provides additional functionality for SGD, for example to enable users to access the drives on their client device.
- The component installed on *client devices* enables users to connect to an SGD server.

Topics in this chapter include the following:

- [“Performing the Installation” on page 11](#)
- [“Installing the SGD Enhancement Module for Microsoft Windows” on page 14](#)
- [“Installing the SGD Enhancement Module for UNIX and Linux Platforms” on page 15](#)
- [“Installing the SGD Client Manually” on page 18](#)

---

## Performing the Installation

On Solaris Operating System (Solaris OS) platforms, install SGD with the `pkgadd` command.

On Linux platforms, install SGD with the `rpm` command.

By default, SGD is installed in the `/opt/tarantella` directory. You can change the installation directory as follows:

- **Solaris OS platforms** – The installation program asks you for the installation directory when you install the software.
- **Solaris 10 OS Trusted Extensions platforms** – The installation program asks you for the installation directory when you install the software. You *must* select another installation directory because the `/opt` directory is a read-only directory. You must also install SGD in a labelled zone. Do not install SGD in the global zone.
- **Linux platforms** – You can choose a different installation directory by using the `--prefix` option with the `rpm` command when you install the software.

Once you install SGD, the SGD server and the SGD web server are running.

## ▼ How To Install SGD




---

**Caution** – If you are upgrading from a release before SGD version 4.40, this release contains significant changes to the SGD organizational hierarchy. Read [“Organizational Changes for Versions 4.40 and Later” on page 21](#) before you upgrade.

---

### 1. Obtain the software.

Download the software from <http://www.sun.com/software/products/sgd> or copy it from the installation media.

Save the software to a temporary directory on the host.

These are the package files:

- `tta-version.sol-x86.pkg` for Solaris OS on x86 platforms
- `tta-version.sol-sparc.pkg` for Solaris OS on SPARC® technology platforms
- `tta-version.i386.rpm` on Linux platforms

### 2. Log in as superuser (root) on the host.

### 3. Install SGD.

If the package file is compressed, you must expand it before installing.

To install on Solaris OS on x86 platforms:

```
# pkgadd -d /tmpdir/tta-version.sol-x86.pkg
```

To install on Solaris OS on SPARC technology platforms:

```
# pkgadd -d /tmpdir/tta-version.sol-sparc.pkg
```

---

**Note** – On Solaris OS platforms, if the installation fails with a `pwd: cannot determine current directory!` error message, change to the `/tmpdir` directory and try again.

---

To install on Linux platforms:

```
# rpm -Uvh /tmpdir/tta-version.i386.rpm
```

#### 4. Verify that the SGD package is registered in the package database.

On Solaris OS platforms:

```
# pkginfo -x tta
```

On Linux platforms:

```
# rpm -q tta
```

#### 5. Start the SGD server.

```
# /opt/tarantella/bin/tarantella start
```

The first time you start the SGD server, the SGD installation program runs. This program does the following:

- Asks you to agree to the Software License Agreement.
- Presents a list of recommended settings that you can accept or change, including the following:
  - **TCP port.** If another process is currently running on Transmission Control Protocol (TCP) port 80, the SGD installation program asks you which TCP port to use for the SGD web server.
  - **Peer DNS name.** You must use a fully-qualified Domain Name System (DNS) name. If you are running SGD on a network with a firewall, use the DNS name that the host is known by inside the firewall.
- Installs and configures the software. This includes creating an organizational hierarchy with some sample applications, and making the UNIX® or Linux system root user an SGD Administrator.
- Adds a file to the system startup directory to ensure that the SGD server and the SGD web server start when the system reboots. For example, if you install the software in run level 3, the file is in the `/etc/rc3.d` directory and named `*sun.com-sgd-base`.
- Modifies root's crontab to archive the SGD log files weekly.

- On Linux platforms only, adds an SGD Pluggable Authentication Module (PAM) configuration file, `/etc/pam.d/tarantella`. This is copied from the existing `/etc/pam.d/passwd` file. If this file does not exist, the PAM configuration file is not created.
- Creates a log file, `/tmp/tta_inst.log`. This file contains a copy of the messages displayed during installation.

---

## Installing the SGD Enhancement Module for Microsoft Windows

The SGD Enhancement Module for Microsoft Windows contains modules for advanced load balancing, client drive mapping (CDM), and seamless windows. When you install the Enhancement Module, you can choose which of these modules to install.

By default, the Enhancement Module is installed in the `C:\Program Files\Tarantella\Enhancement Module` directory, but the installation program asks you for the installation directory.

After installation, the load balancing service is running. The load balancing service starts automatically whenever the Windows host is rebooted.

### ▼ How to Install the SGD Enhancement Module for Microsoft Windows

1. **Log in to the Windows host as a user with administrator privileges.**
2. **Save the Enhancement Module installation program to a temporary directory on the host.**

If you are installing from the installation media, the installation program is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from `http://server.example.com`, where `server.example.com` is the name of an SGD server. When the SGD web server Welcome Page displays, click **Install a Sun Secure Global Desktop Enhancement Module**.

The SGD Enhancement Module installation program is `temwin32.exe`.

3. **Install the SGD Enhancement Module.**

Double-click `temwin32.exe` and follow the instructions on the screen.

---

# Installing the SGD Enhancement Module for UNIX and Linux Platforms

The SGD Enhancement Module for UNIX and Linux Platforms contains modules for advanced load balancing, CDM and UNIX audio.

The UNIX audio module of the Enhancement Module is optional and is not installed by default. If you choose to install the UNIX audio module, the SGD audio driver is installed in the kernel of the operating system.

On Solaris OS platforms, the UNIX audio module can be installed only in the global zone.

On Linux platforms, the UNIX audio module can be installed only if your kernel version is 2.4.20 or later. The SGD audio driver is compiled before it is installed in the kernel. To compile the audio driver, the following must be available on the host:

- Header files for your Linux kernel version
- GNU Compiler Collection (GCC)
- make utility
- soundcore kernel module

On Solaris OS platforms, install the Enhancement Module with the `pkgadd` command.

On Linux platforms, install the Enhancement Module with the `rpm` command.

By default, the Enhancement Module is installed in the `/opt/tta_tem` directory. You can change the installation directory as follows:

- **Solaris OS platforms** – The installation program asks you for the installation directory when you install the software.
- **Solaris 10 OS Trusted Extensions platforms** – The installation program asks you for the installation directory when you install the software. You *must* select another installation directory because the `/opt` directory is a read-only directory. You must also install the Enhancement Module in a labelled zone. Do not install the Enhancement Module in the global zone.
- **Linux platforms** – You can choose a different installation directory by using the `--prefix` option with the `rpm` command when you install the software.

After installation, the advanced load balancing module and the UNIX audio module, if selected, are running. The CDM module is not running, because this requires additional configuration. The additional configuration needed is described in the *Sun Secure Global Desktop 4.5 Administration Guide*.

The Enhancement Module installation program adds a file to the system startup directory to ensure that the Enhancement Module starts when the system reboots. For example, if you install the software in run level 3, the file is in the `/etc/rc3.d` directory and named `*sun.com-sgd-em`.

## ▼ How To Install the SGD Enhancement Module on Solaris Platforms

### 1. Save the SGD Enhancement Module to a temporary directory on the host.

If you are installing from the installation media, the package is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from `http://server.example.com`, where *server.example.com* is the name of an SGD server. When the SGD web server Welcome Page displays, click Install a Sun Secure Global Desktop Enhancement Module.

These are the package files:

- `tem-version.sol-x86.pkg` for Solaris OS on x86 platforms
  - `tem-version.sol-sparc.pkg` for Solaris OS on SPARC technology platforms
- where *version* is the SGD version number.

### 2. Log in as superuser (root) on the host.

### 3. Install the SGD Enhancement Module.

If the package file is compressed, you must expand it before installing.

To install on Solaris OS on x86 platforms:

```
# pkgadd -d /tempdir/tem-version.sol-x86.pkg
```

To install on Solaris OS on SPARC technology platforms:

```
# pkgadd -d /tempdir/tem-version.sol-sparc.pkg
```

When you install, the Enhancement Module installation program presents the following settings that you can accept or change:

- The installation directory.
- The amount of virtual memory the host has. This is used for load balancing.
- Whether to install the UNIX audio module.

4. Verify that the Enhancement Module package is registered in the package database.

```
# pkginfo -x tem
```

## ▼ How To Install the SGD Enhancement Module on Linux Platforms

1. Save the SGD Enhancement Module to a temporary directory on the host.

If you are installing from the installation media, the package is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from `http://server.example.com`, where *server.example.com* is the name of an SGD server. When the SGD web server Welcome Page displays, click Install a Sun Secure Global Desktop Enhancement Module.

The package files are `tem-version.i386.rpm`, where *version* is the SGD version number.

2. Log in as superuser (root) on the host.

3. Install the SGD Enhancement Module.

```
# rpm -Uvh tem-version.i386.rpm
```

4. Verify that the Enhancement Module package is registered in the package database.

```
# rpm -q tem
```

5. Start the Enhancement Module installation program.

```
# /opt/tta_tem/bin/tem start
```

6. Configure settings for the Enhancement Module.

The Enhancement Module installation program presents the following settings that you can accept or change:

- The amount of virtual memory the host has. This is used for load balancing.
- Whether to install the UNIX audio module.

# Troubleshooting Installing the UNIX Audio Module on Linux Platforms

On Linux platforms, if the UNIX audio module does not install, the SGD Enhancement Module installation program asks you whether to cancel the installation or to continue the installation without installing the UNIX audio module. If the UNIX audio module does not install, check the following:

- Is the Linux kernel version 2.4.20 or later?
- Are the header files for your Linux kernel version installed?
- Do the version numbers of the header files and the Linux kernel match?
- Does the GCC version match the version used to compile the Linux kernel?
- Does the `dmesg` utility reveal any other errors?

---

## Installing the SGD Client Manually

The SGD Client is usually installed automatically when a user connects to an SGD server using a browser with Java™ technology enabled. Follow these instructions only if you want to install the SGD Client *manually*.

You do not need superuser (root) or administrator privileges to install the SGD Client.

On Microsoft Windows platforms, the SGD Client is installed in the `C:\Program Files\Sun\Secure Global Desktop Client` directory by default, but you can choose a different installation directory when you install the software. A shortcut for the SGD Client is added to the Windows Start Menu.

On UNIX and Linux platforms, the SGD Client is installed in the `$HOME/bin` directory by default, but you can choose a different installation directory when you install the software.

## ▼ How to Install the SGD Client Manually on Microsoft Windows Platforms

### 1. In a browser, go to an SGD web server.

For example, `http://server.example.com`, where `server.example.com` is the name of an SGD server.

The SGD web server Welcome Page displays.

**2. (Optional) Select your preferred language.**

Click one of the flags at the top of the Welcome Page.

The Welcome page displays in the selected language.

**3. Click Install the Sun Secure Global Desktop Client.**

The Sun Secure Global Desktop Client page displays.

**4. Download the SGD Client installation program.**

Click Download the Secure Global Desktop Client for Microsoft Windows.

Save the installation program to a temporary directory on the PC.

The SGD Client installation program is `sgdcwin-lang.exe`.

**5. Change to the temporary directory and install the SGD Client.**

Double-click `sgdcwin-lang.exe` and follow the instructions on the screen.

## ▼ How to Install the SGD Client Manually on Solaris OS and Linux Platforms

**1. In a browser, go to an SGD web server.**

For example, `http://server.example.com`, where `server.example.com` is the name of an SGD server.

The SGD web server Welcome Page displays.

**2. (Optional) Select your preferred language.**

Click one of the flags at the top of the Welcome Page.

The Welcome page displays in the selected language.

**3. Click Install the Sun Secure Global Desktop Client.**

The Sun Secure Global Desktop Client page displays.

**4. Download the SGD Client tar file.**

Click Download the Secure Global Desktop Client for *platform*.

Save the tar file to a temporary directory on the host.

Tar file names indicate a platform, as follows:

- `sgdci3so.tar` for Solaris OS on x86 platforms
- `sgdcspso.tar` for Solaris OS on SPARC technology platforms
- `sgdci3li.tar` for Linux platforms

5. Change to the temporary directory and extract the tar file.

```
$ cd /tmpdir
$ tar xvf tarfile
```

6. Install the SGD Client.

```
$ sh sgdc/install
```

Follow the instructions on the screen.

## Logging in Using the SGD Client

- On UNIX and Linux platforms, you start the SGD Client with the `ttatcc` command.
- On Microsoft Windows platforms, you can either start the Client as part of the installation or click Start → Programs → Sun Secure Global Desktop → Login.

The first time you start the SGD Client, it asks for the following information:

- The Uniform Resource Locator (URL) of the SGD server to connect to. This is usually `http://server.example.com/sgd`, where *server.example.com* is the name of an SGD server.
- The proxy settings to use. The settings can be determined from your default browser, if Java technology is enabled, or you can type them in.

# Upgrading SGD

---

This chapter describes the requirements and procedures for upgrading from a previous version of Sun Secure Global Desktop (SGD).

Topics in this chapter include the following:

- [“Before You Upgrade” on page 21](#)
- [“Performing the Upgrade” on page 24](#)
- [“Upgrading Other SGD Components” on page 28](#)

---

## Before You Upgrade

This section describes the things you must know and do before upgrading.

## Organizational Changes for Versions 4.40 and Later

SGD version 4.40 introduced a new web-based administration tool, the Administration Console, which replaced Object Manager, Array Manager, Configuration Wizard, and Session Manager. As a result, if you are upgrading from a release before version 4.40 there are some significant changes to the SGD organizational hierarchy. The main changes are as follows:

- Application objects are always created and maintained in a new organization object called `o=applications`.
- Application server objects, formerly known as host objects, are always created and maintained in a new organization object called `o=appservers`.

- The previous administration tools allowed you to build complex relationships between objects. The allowed relationships have been simplified.

When you upgrade from a release before version 4.40, your existing application and application server objects, and their associated group and organizational unit objects, are moved to the new organizations. As far as possible, SGD attempts to preserve the relationships between the objects, but after the upgrade some users might find that some applications are no longer on their webtop.

Before you upgrade from a release before version 4.40, it is advisable to perform a test to see how the changes affect you. You can do this by upgrading a pre-production environment that mirrors the production environment. Alternatively, detach a secondary server from the array and upgrade it.

## Upgrades and Early Access Program Software

Upgrades to or upgrades from Early Access Program (EAP) software releases of SGD are not supported. EAP software releases must always be a fresh installation.

## Conditions for Upgrading

Upgrades to this version of SGD are only supported from the following versions:

- Sun Secure Global Desktop Software version 4.41
- Sun Secure Global Desktop Software version 4.40

If you want to upgrade from any other version of SGD contact Sun Support.

If you are sure you want to perform an unsupported upgrade, you must create an empty file `/opt/tarantella/var/UPGRADE` before installing the new version of the software. Your SGD installation might not be upgraded correctly.

## Before You Upgrade on Solaris OS Platforms

When you upgrade on Solaris™ Operating System (Solaris OS) platforms, the `pkgadd` command performs several checks and asks you to confirm the changes before installing the package. You can create an administration file that instructs `pkgadd` to bypass these checks and install the package without user confirmation.

To avoid user interaction, the administration file must contain the following lines:

```
conflict=nocheck
instance=unique
```

When you upgrade SGD, use the `pkgadd -a adminfile` command to specify the administration file.

If you do not specify an administration file when you upgrade, the SGD installation program creates one for you and gives you the option to quit the installation so that you can run the `pkgadd` command again with the `-a adminfile` option.

## Upgrades and Your Existing Configuration

When you upgrade, the following changes are applied to your existing configuration:

- Your existing Enterprise Naming System (ENS) database is preserved and backed up.

The ENS database is the storage area for all the objects in your SGD organizational hierarchy.

The `/opt/tarantella/var/ens` directory is backed up to the `/opt/tarantella/var/ens.oldversion` directory.

The backup is not changed. The existing ENS database might be changed if changes are needed to enable it work with the new version of SGD.

---

**Note** – “[Organizational Changes for Versions 4.40 and Later](#)” on page 21 has details of some significant changes to ENS in this release.

---

- The SGD server configuration and the SGD global configuration are preserved but *not* backed up.

This configuration is stored in the `/opt/tarantella/var/serverconfig` directory.

This configuration is changed only if new properties files need to be added or new attributes need to be added to existing properties.

- All the server resources files in the `/opt/tarantella/var/serverresources` directory are replaced.

These files are not normally edited as they control how SGD works.

- Your SGD login scripts are preserved and backed up.

The `/opt/tarantella/var/serverresources/expect` directory is backed up to `/opt/tarantella/var/serverresources/expect.oldversion`.

- Your customized SGD files are backed up but they are *not upgraded*.

You can customize SGD by *changing the files* found in a standard installation, for example webtop themes, or by *adding your own files*, for example login scripts.

You have to upgrade these files manually.

When you install the new version of SGD, the installation program warns you if files exist that might need to be upgraded manually. See [“Upgrading a Customized SGD Installation” on page 26](#) for advice on how to upgrade these files.

---

## Performing the Upgrade

How you upgrade SGD depends on whether you are upgrading an evaluation version or a fully licensed version of SGD, and on whether you are upgrading a single-server or multiple-server array. If you have customized SGD, you might have to upgrade your customized files manually.

### Upgrading Evaluation Versions of SGD

If an SGD server does not have a license key installed, or belong to an array that is fully licensed, the SGD server is in *evaluation mode*. After 30 days the evaluation period expires and the SGD server is in *expired evaluation mode*.

Upgrade an SGD server in evaluation mode or expired evaluation mode by installing the next version of the software.

An SGD server that was in expired evaluation mode remains in expired evaluation mode after the upgrade. You cannot log in to an SGD server when it is in expired evaluation mode.

To license a server when it is in expired evaluation mode, you must either use the `tarantella license add` command to add a valid license key, or join the server to an array that is already fully licensed.

### ▼ How to Upgrade a Fully Licensed Single-Server Array

1. **Make sure no user sessions and application sessions are running in the array, including suspended sessions.**
2. **Upgrade the server by installing the new version of SGD.**

## ▼ How to Upgrade a Fully Licensed Multiple-Server Array

All SGD servers in a multiple-server array must run on the same version of the SGD software. This means that to upgrade an array, you must dismantle the array, upgrade each server independently, and then rebuild the array.

1. **Make sure no user sessions and application sessions are running in the array, including suspended sessions.**
2. **Dismantle the array.**

On the *primary SGD server*, detach the secondary SGD servers from the array:

```
# tarantella array detach --secondary server
```



---

**Caution** – Detach only one secondary SGD server at a time. After making the change to the structure of the array, wait until SGD has copied the change to all the SGD servers in the array before making any further changes. Run the `tarantella status` command on the primary SGD server to check the status of the array.

---

When a secondary SGD server is detached from an array, it loses its license keys and, temporarily, you might not be able to log in to SGD on this host.

3. **Upgrade the primary SGD server by installing the new version of the software.**
4. **Upgrade the secondary SGD servers by installing the new version of the software.**
5. **Rebuild the array.**

On the *primary SGD server*, add the secondary SGD servers to the array:

```
# tarantella array join --secondary server
```



---

**Caution** – Add only one secondary SGD server at a time. After making the change to the structure of the array, wait until SGD has copied the change to all the SGD servers in the array before making any further changes. Run the `tarantella status` command on the primary SGD server to check the status of the array.

---

When a secondary SGD server is added to an array, it gains any license keys installed on the primary SGD server.

# Upgrading a Customized SGD Installation

When you upgrade, the SGD installation program preserves the customized files it finds, but it does not upgrade them. These files have to be manually upgraded. Two sets of files might need to be upgraded:

- **SGD web server files** – Web application files and files used to configure the SGD web server
- **SGD server files** – Files used by the SGD server, such as login scripts

Two types of customized files might need attention after you have upgraded:

- **Customized files** – Files found in a standard SGD installation that have been changed by an SGD Administrator
- **Bespoke files** – Files your organization created and added to an SGD installation

## Upgrading Customized SGD Web Server Files

When you upgrade, the SGD installation program backs up any *customized* SGD web server files it detects. Backed-up files and their locations are listed in the `/opt/tarantella/var/log/webservercustomized.list` log file.

To upgrade the customized files, use utilities such as `diff` and `patch` to compare and merge the differences between the backed-up files and the files in the standard SGD installation.

The SGD installation program copies any *bespoke* SGD web server files it finds into the new installation. These files are not changed.

## Upgrading Customized SGD Server Files

When you upgrade, the SGD installation program backs up the customized and bespoke SGD server files it detects and produces the following log files:

- `/opt/tarantella/var/log/upgraded.files` – A summary of the changes
- `/opt/tarantella/var/log/customized.list` – A list of any files that an Administrator has edited or added
- `/opt/tarantella/var/log/customizedchanged.list` – A list of any files that an Administrator has edited that were changed by the upgrade
- `/opt/tarantella/var/log/docrootjava.log` – A list of new or modified Java™ technology files from the original installation

Use these log files to identify the files that need to be manually upgraded.

## ▼ How to Manually Upgrade Customized SGD Server Files

### 1. Create a copy of the customized file.

### 2. Identify the changes made between SGD versions.

The `customizedchanged.list` log file lists the customized files that have to be manually upgraded. For each file listed in this log file, your system will have three versions of the file:

- The old, customized version in one of the following directories:
  - `/opt/tarantella/var/serverresources.oldversion` for login scripts.
  - `/opt/tarantella/etc/data.oldversion` for other files such as color maps.
- The old, uncustomized version in the `/opt/tarantella/etc/templates.oldversion` directory.
- The new, uncustomized version in the `/opt/tarantella/etc/templates` directory.

Use a utility such as `diff` to compare the old, uncustomized file with the new, uncustomized file. This highlights the changes made between SGD versions.

### 3. Apply the changes to the customized file.

Use a utility such as `patch` to apply the changes identified in [Step 2](#) to the copy of your customized file.

### 4. Copy the upgraded customized file into the correct location in the new SGD installation.

## ▼ How to Manually Upgrade Bespoke SGD Server Files

### 1. Create a copy of the bespoke file.

### 2. Identify the changes made between SGD versions.

The `docrootjava.log` and `customized.list` log files list the bespoke files that might have to be manually upgraded.

The only way to upgrade bespoke files is to compare versions of the standard SGD files to identify changes that have taken place and then apply those changes to your bespoke files.

Use a utility such as `diff` to compare the old, uncustomized file with the new, uncustomized file. This highlights the changes made between SGD versions.

To identify the changes, compare the following files:

- The old version of the standard SGD files in the `/opt/tarantella/etc/templates.oldversion` directory.
- The new version of the standard SGD files in the `/opt/tarantella/etc/templates` directory.

**3. Apply the changes to the bespoke file.**

Use a utility such as `patch` to apply the changes identified in Step 2 to the copy of your bespoke file.

**4. Copy the upgraded bespoke file into the correct location in the new SGD installation.**

---

## Upgrading Other SGD Components

This section describes how you upgrade the SGD Enhancement Module and the SGD Client.

### ▼ How to Upgrade the SGD Enhancement Module for Microsoft Windows

- **Install the new version of the SGD Enhancement Module.**

See [“How to Install the SGD Enhancement Module for Microsoft Windows” on page 14.](#)

### ▼ How to Upgrade the SGD Enhancement Module for UNIX<sup>®</sup> and Linux Platforms

When you upgrade the SGD Enhancement Module and you install the UNIX audio module, you might see a message that says the UNIX audio module is already running. This message is displayed because the SGD audio driver is currently in use and cannot be stopped. As the SGD audio driver has not changed in this release, this message can be safely ignored.

- **Install the new version of the Enhancement Module.**

See [“Installing the SGD Enhancement Module for UNIX and Linux Platforms” on page 15.](#)

### ▼ How to Upgrade the SGD Client Automatically

The SGD Client can only be upgraded automatically if *both* of the following are true:

- The previous version of the SGD Client was installed automatically
  - The user's browser has a supported Java™ Plugin tool and Java technology is enabled
1. **Close any existing browser sessions.**
  2. **Start a new browser session.**
  3. **Log in to SGD.**  
See ["How to Log In to SGD"](#) on page 31.

## ▼ How to Upgrade the SGD Client Manually

Follow this procedure only if the previous version of the SGD Client was installed manually.

- **Install the new version of the SGD Client.**  
See ["Installing the SGD Client Manually"](#) on page 18.



## Getting Started With SGD

---

This chapter describes how to log in to Sun Secure Global Desktop (SGD) and get started using the software.

Topics in this chapter include the following:

- [“Logging In to SGD” on page 31](#)
- [“Using the Webtop” on page 34](#)
- [“SGD Administration Tools” on page 37](#)
- [“Creating Users” on page 42](#)
- [“Adding Applications to Webtops” on page 49](#)
- [“Managing SGD” on page 62](#)
- [“Controlling SGD” on page 67](#)
- [“SGD Network Architecture” on page 69](#)
- [“Next Steps” on page 70](#)

---

## Logging In to SGD

SGD supports several mechanisms for authenticating users. By default, any user with an account on the SGD host can log in to SGD using their UNIX® or Linux system user name and password.

### ▼ How to Log In to SGD

To use SGD, you need the SGD Client and a supported browser. Usually the SGD Client is installed automatically when you log in. To perform an automatic installation, the browser must have a supported Java™ Plugin tool and Java™

technology must be enabled. If you are using Internet Explorer on Microsoft Windows Vista platforms, you must also add the Uniform Resource Locator (URL) of the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

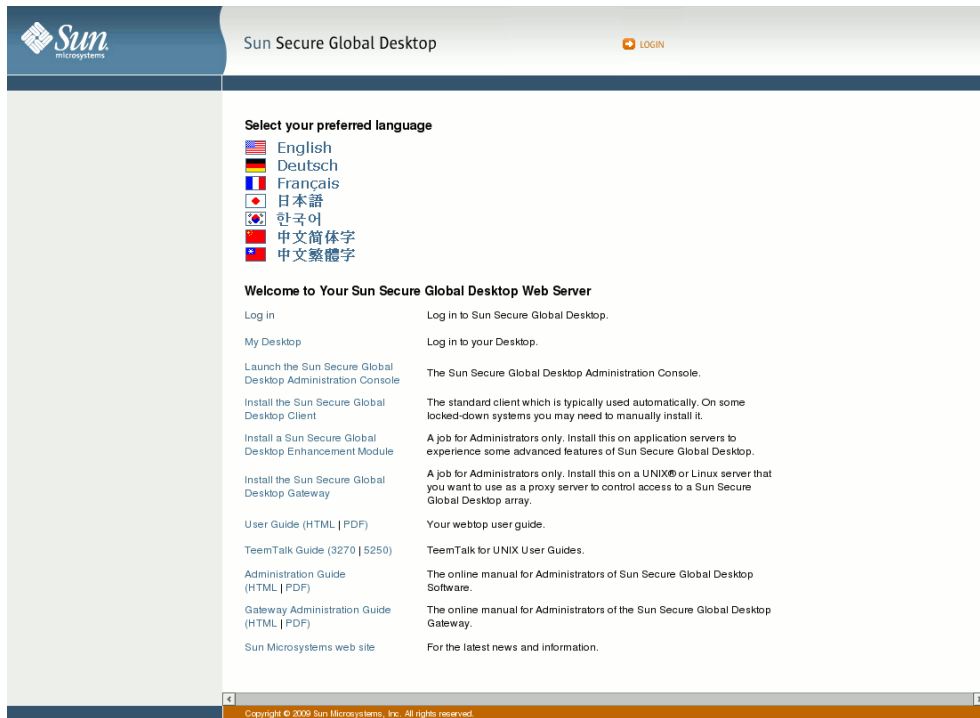
If your browser does not have Java technology, you must manually install the SGD Client and then connect to SGD. See ["Installing the SGD Client Manually" on page 18](#).

To use SGD with a browser, the browser must have the JavaScript™ programming language enabled.

**1. Using a browser, go to `http://server.example.com` where `server.example.com` is the name of an SGD server.**

The SGD web server Welcome Page is displayed, as shown in [FIGURE 4-1](#).

**FIGURE 4-1** The SGD web server Welcome Page



**2. (Optional) Select your preferred language.**

Click one of the flags at the top of the Welcome page.

The Welcome Page is displayed in the selected language.

### 3. Click Login.

The SGD Login Page is displayed, as shown in [FIGURE 4-2](#).

### 4. Log in.

When you install SGD, SGD creates a default SGD Administrator with the user name “Administrator”. This user authenticates using the password of the UNIX or Linux system root user on the host.

Type Administrator for the Username and the superuser (root) password for the Password.

**FIGURE 4-2** The SGD Login Page



If a Java technology security message displays, click Run to install the SGD Client.

The Untrusted Initial Connection message is displayed. See [FIGURE 4-3](#).

**FIGURE 4-3** An Untrusted Initial Connection message



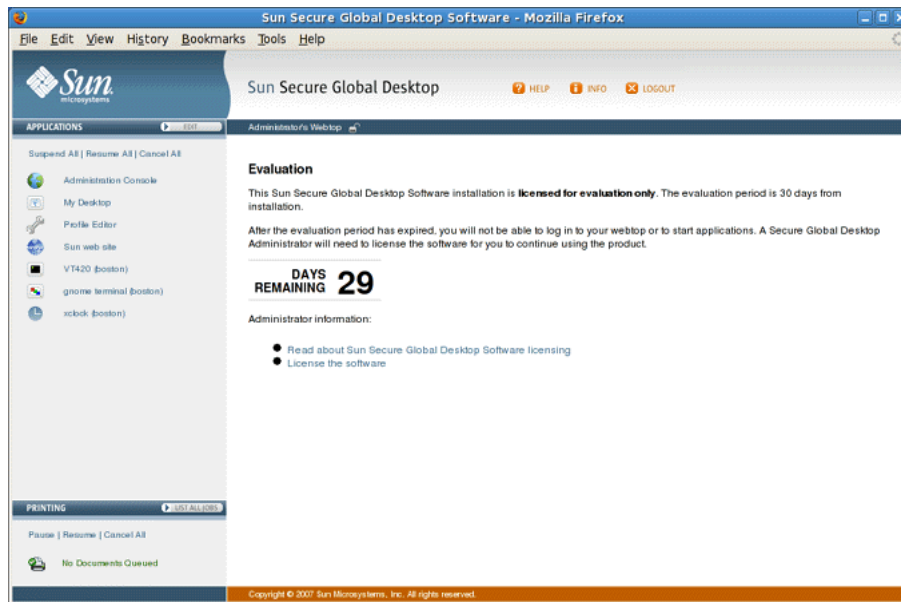
### 5. Check the Untrusted Initial Connection message.

The Untrusted Initial Connection message is a security measure to ensure the SGD Client only connects to trusted hosts. The message gives you the opportunity to check the host name and server certificate details before agreeing to the connection. The message displays only once for each SGD server to which you connect.

Check that the host details are correct. If they are, click Yes. If they are not, click No.

The webtop for the Administrator user is displayed, as shown in [FIGURE 4-4](#).

**FIGURE 4-4** The Administrator User's Webtop



The SGD Client icon is displayed in the task bar. See [FIGURE 4-5](#).

**FIGURE 4-5** SGD Client Task Bar Icon



## Using the Webtop

The webtop lists the applications and documents you access through SGD, including the SGD administration tools.

The webtop lists some sample applications that the SGD installation program found on the host so that you can start using SGD.

## Running Applications

To run an application, click its link on the webtop, as shown in [FIGURE 4-6](#).

**FIGURE 4-6** An Application Link on a Webtop

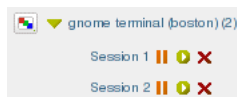


When you start an application, you might be asked for a user name and password. This is authentication information for the application server which is running the application. These details can be cached securely so you do not need to enter them more than once for each application server.

SGD Administrators configure how applications appear. Some applications might appear full-screen with no window decoration, and others in a window that behaves in the same way as a window on the client device.

When an application is running, a triangle appears in front of the application's name on the webtop and a number appears in brackets after it. The session toolbar also appears below the application name, as shown in [FIGURE 4-7](#).

**FIGURE 4-7** The Session Toolbar



The number in brackets is the number of separate instances of the application you have started. SGD Administrators configure how many simultaneous instances of an application that you can run.

Some applications can be configured to keep running even when they are not displayed. These are “resumable” applications. To close an application's window without ending the application, you *suspend* the application. To display the window again and start using the application, you *resume* the application.

There is a separate session toolbar for each running instance of the application, which you use as follows:

- Click the Suspend button to suspend an application session
- Click the Resume button to resume an application session
- Click the Cancel button to end an application session

Click the triangle to hide and show the session toolbars for the application sessions, as shown in [FIGURE 4-8](#).

**FIGURE 4-8** Hidden Session Toolbars



You can manage all your application sessions at once from the links at the top of the Applications area. You use these links as follows:

- Click Suspend All to suspend all running applications
- Click Resume All to resume all suspended application
- Click Cancel All to end all running or suspended applications

Applications can have one of three resumability settings.

Setting	Description
Never	The application exits when you log out of SGD. You cannot suspend or resume, non-resumable applications.
During the User Session	The application continues to run until you log out of SGD. While you are logged in, you can suspend and resume these applications.
General	The application continues to run even after you have logged out of SGD. When you log in again, click the resume button to display the running application again.

Resumable applications are useful for the following reasons:

- Applications that take a long time to start can be left running, even after you have logged out of SGD.
- You can leave applications running while you travel.
- You can easily recover from browser or other crashes.

## Changing Your Settings

If you click the Edit button in the Applications area of the webtop, you can change your settings.

On the Edit Groups tab, you can “personalize” your webtop by arranging your applications into groups. You decide how and when the groups display. Groups are useful for keeping similar applications together or for hiding applications not used very often. Only an SGD Administrator can add an application to, or remove an application from, the list of applications that are available on a user’s webtop.

On the Client Settings tab, you can configure the settings for the SGD Client, for example the proxy server to use, or whether the list of applications you can run displays in the desktop Start or Launch menu. The settings are stored in a profile on the client device.

## Logging Out

You must log out of SGD before closing your browser. This enables SGD to shut down any applications that need not run any more and stop the SGD Client.

If you close your browser without logging out, you are not logged out of SGD, because the SGD Client is still running. If you accidentally close the browser, you can only display the webtop by logging in again.

To log out of SGD, click the Logout button on the webtop and click OK when prompted for confirmation.

---

## SGD Administration Tools

SGD has the following administration tools:

- **Administration Console** – Enables user and user session management, SGD server configuration, and the configuration of applications for SGD users
- **Profile Editor** – Enables definition of settings for the SGD Client for the users in your organization
- **tarantella command** – Enables control and configuration of SGD from the command line

The Administration Console and the Profile Editor are available on the webtop of SGD Administrators.

## The Administration Console

To display the Administration Console, you can use any browser that is supported by SGD, apart from Safari. See the *Sun Secure Global Desktop 4.5 Administration Guide* for details of the supported browsers for SGD. The browser must have the JavaScript programming language enabled.

The Administration Console works best when you run it on the primary SGD server in the array.

## Starting the Administration Console

To start the Administration Console, you click the link on the webtop.

If you want to run the Administration Console without displaying the webtop, you can run it from the following locations:

- <http://server.example.com> and click the Launch the Secure Global Desktop Administration Console link
- <http://server.example.com/sgdadmin>

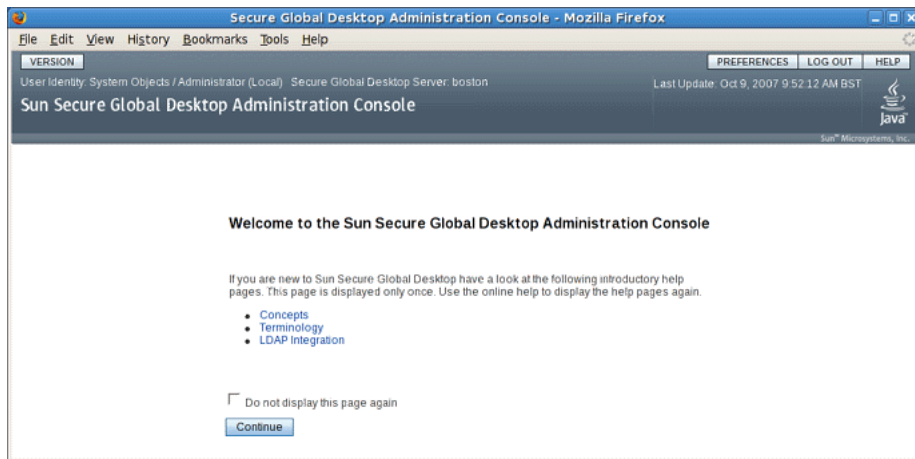
where *server.example.com* is the name of an SGD server.

If you run the Administration Console without displaying a webtop, you are prompted to log in as an SGD Administrator.

## Using the Administration Console

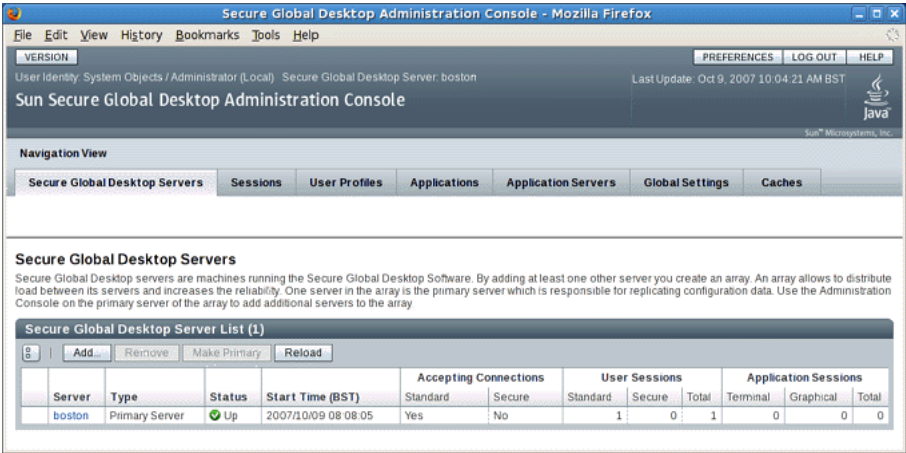
When you log in to the Administration Console, the Welcome screen is displayed, as shown in [FIGURE 4-9](#).

**FIGURE 4-9** The Administration Console Welcome Screen



The Welcome Screen contains links to information to help you get started. Click Continue to display the Administration Console. The Administration Console opens in Navigation View, as shown in [FIGURE 4-10](#).

**FIGURE 4-10** The Administration Console in Navigation View



Navigation View is the “top-level” view that enables you to access the tabs for managing the different areas of SGD. The following table summarizes the tabs available in Navigation View and what they are used for.

Tab	Description
Secure Global Desktop Servers	Managing and configuring SGD servers. If you upgraded from a previous release of SGD, this tab replaces Array Manager. This tab is described in more detail in <a href="#">“Managing SGD” on page 62</a> .
Sessions	Managing users’ SGD sessions and application sessions. If you upgraded from a previous release of SGD, this tab replaces Session Manager. This tab is described in more detail in <a href="#">“Monitoring Users” on page 65</a> .
User Profiles	Managing and configuring users’ SGD settings. If you upgraded from a previous release of SGD, this tab replaces Object Manager. This tab is described in more detail in <a href="#">“Creating Users” on page 42</a> .
Applications	Managing and configuring the applications that users can run through SGD. If you upgraded from a previous release of SGD, this tab replaces Object Manager. This tab is described in more detail in <a href="#">“Adding Applications to Webtops” on page 49</a> .

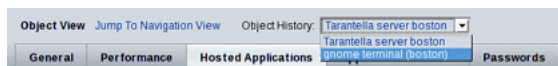
Tab	Description
Application Servers	<p>Managing and configuring the application servers that run the applications displayed through SGD.</p> <p>If you upgraded from a previous release of SGD, this tab replaces Object Manager.</p> <p>This tab is described in more detail in <a href="#">“Adding Applications to Webtops” on page 49.</a></p>
Global Settings	<p>Configuring settings that apply to SGD as a whole.</p> <p>If you upgraded from a previous release of SGD, this tab replaces Array Manager.</p> <p>This tab is described in more detail in <a href="#">“Managing SGD” on page 62.</a></p>
Caches	<p>Managing the application server passwords and authentication tokens that SGD has stored.</p>

SGD is built on the following principles of directory services:

- Users, applications, and application servers are represented by *objects* in a directory. The objects are organized into an *organizational hierarchy* representing your organization.
- Different types of object have different configuration settings, known as *attributes*.
- The *relationships* between objects are important and have meanings.
- Each object is identified using a *unique name*.

SGD includes a number of different object types. When you select an object to work with, the Administration Console changes to Object View. The Administration Console provides links to enable you to switch between Object View and Navigation View, and also an Object History that enables you to switch between the objects you have recently worked with, as shown in [FIGURE 4-11](#).

**FIGURE 4-11** The Administration Console Navigation Links

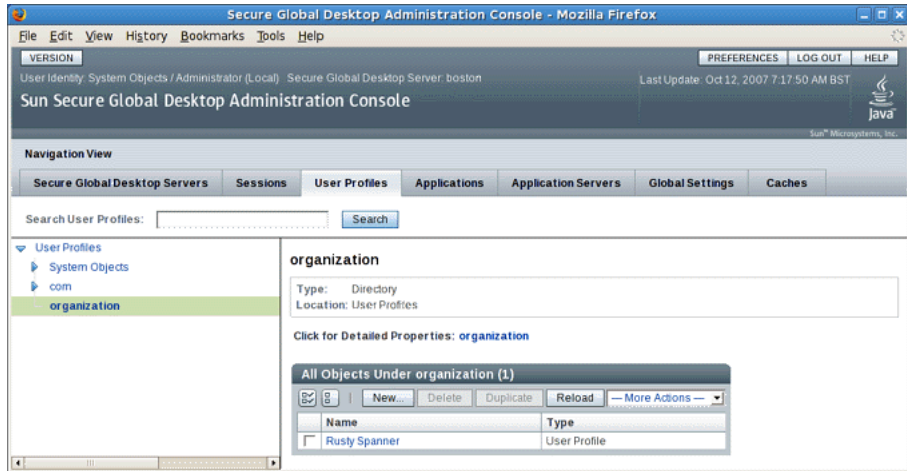


**Caution** – When using the Administration Console, do not use the browser’s Back button. Instead, use the navigation links to move between pages in the Administration Console.

The User Profiles, Applications, and Application Servers tabs are divided into two sections. On the left is the navigation tree and on the right is the content area, as shown in [FIGURE 4-12](#). The navigation tree only shows the container objects that are

used to structure your organizational hierarchy. As you browse and select objects in the navigation tree, the content area displays a list of objects contained in the selected object.

**FIGURE 4-12** The Navigation Tree and Content Area



Several of the tabs and screens in the Administration Console have a search field. The search is case insensitive and accepts only the \* wildcard character. The search results are displayed in a table and are limited to a maximum of 150 hits.

Most tabs in the Administration Console present information in tables. Often the information in a table cell is a link that can be clicked to display further information.

## The tarantella Command

The tarantella command is a script installed in the *install-dir/bin* directory. By default, *install-dir* is */opt/tarantella*. As this script is not on the standard PATH, you must use the full path each time you run the command, or change to */opt/tarantella/bin* before running the command. Alternatively, do the following:

- Add */opt/tarantella/bin* to the PATH, for example:  

```
PATH=$PATH:/opt/tarantella/bin; export PATH
```
- Create an alias, for example:  

```
alias t=/opt/tarantella/bin/tarantella
```

The `tarantella` command is actually a family of commands, each of which can have its own set of subcommands. You always run the subcommands through the `tarantella` command, for example:

```
# tarantella license list
```

Help is available for every command by using the `--help` command-line argument.

Many commands are designed so that you can build scripts around them.

The following restrictions apply as to which users can use particular `tarantella` commands:

- Commands that control the SGD server and SGD web server can be run only by superuser (root)
- Commands for creating and managing arrays of SGD servers can be run only by SGD Administrators
- All other commands can be run by any user in the `ttaserv` group

Use the `usermod -G` command to make a user a member of the `ttaserv` group. The `ttaserv` group does not have to be the user's primary or effective group.

---

## Creating Users

This section describes how to use the Administration Console to create an SGD user. You do this by creating a user profile object. A user profile is used to control a user's SGD settings, such as whether they can log in to SGD and the applications that they can run. This section also describes how to make a user an SGD Administrator.

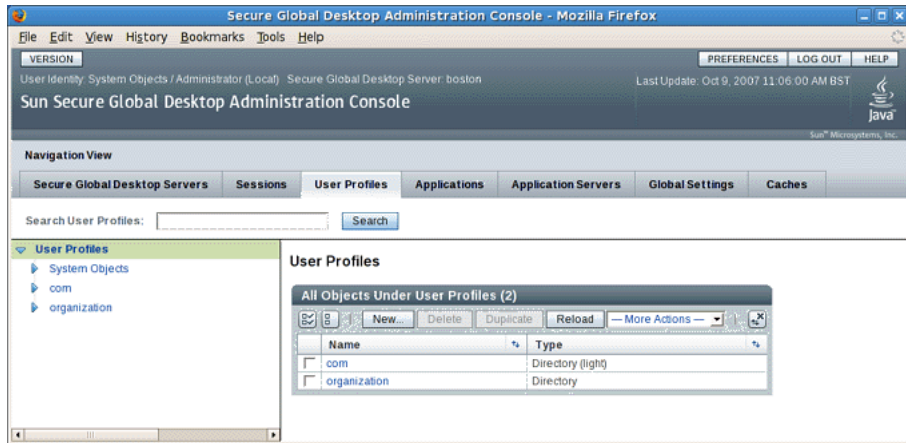
---

**Tip** – You can configure SGD to use a Lightweight Directory Access Protocol (LDAP) directory for obtaining information about users. If you configure SGD for LDAP integration, you do not have to create user profiles. The *Sun Secure Global Desktop 4.5 Administration Guide* has details of how to configure SGD for LDAP integration.

---

In the Administration Console, the User Profiles tab is where you create and manage user profiles. See [FIGURE 4-13](#).

**FIGURE 4-13** The User Profiles Tab



By default, this tab contains two “top-level” objects, a Directory object called organization (o=organization on the command line) and a Directory (light) object called com (dc=com on the command line). You can rename or delete these objects, or create new top-level objects. You create all the objects you need for managing users within these top-level object types.

You can use other Directory objects to subdivide your organization. For example, you might want to use a Directory (organizational unit) for each department in your organization.

## Creating User Profiles and SGD Administrators

In this section, you learn how to create a user profile for yourself, and how to make yourself an SGD Administrator. SGD Administrators always have a user profile. Only SGD Administrators can create user profiles.

Users who occupy the Global Administrators role are SGD Administrators. SGD Administrators can configure SGD using any of the SGD administration tools. Users who do not occupy the Global Administrators role have no administration privileges.

The Global Administrators role is an object in the System Objects organization on the User Profiles tab. The Global Administrators role object is used to assign users administrative privileges and to give them access to the administration tools.

After following these procedures, you can log in to SGD using your UNIX or Linux system user name and password, and run the Administration Console.

You can also use the `tarantella object new_person` command to create a user profile, and the `tarantella role add_member` command to add an SGD Administrator.

## ▼ How to Create a User Profile

1. In the Administration Console, click the User Profiles tab.

2. Select an object in the organizational hierarchy.

Use the navigation tree to select the organization object, as shown in [FIGURE 4-14](#).

You can move your user profile to a different location later if needed.

**FIGURE 4-14** The Organization Object Selected



3. Create the user profile object.

a. In the content area, click New.

The Create a New Object window displays.

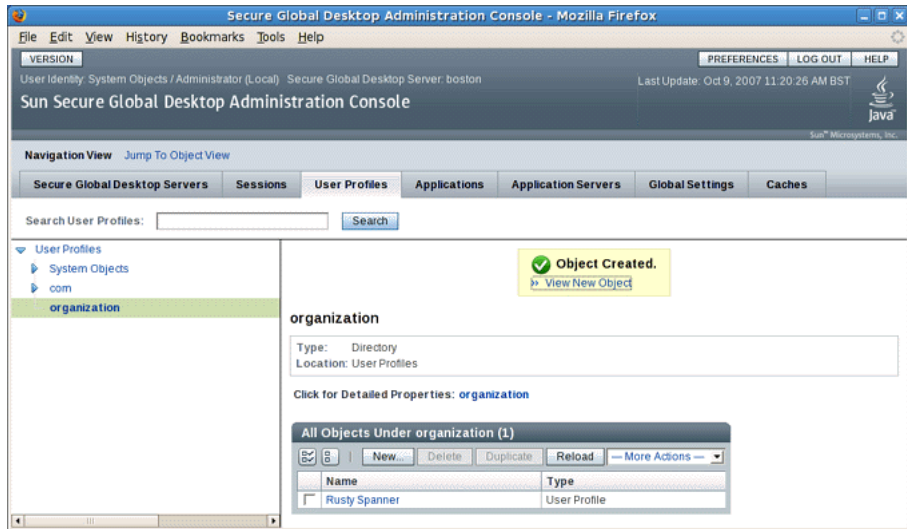
b. In the Name field, type your name.

For example, Rusty Spanner.

c. Ensure that the User Profile option is selected and click Create.

The Create a New Object window closes and the content area is updated with the new object. See [FIGURE 4-15](#).

**FIGURE 4-15** A Newly-Created User Profile



**4. Click the View New Object link.**

The General tab for the user profile displays in Object View. See [FIGURE 4-16](#).

**5. Configure the user profile.**

**a. In the Surname field, type your family name.**

For example, Spanner.

**b. Ensure the Login check box is selected and that the Multiple check box is not selected.**

This ensures that you can log in to SGD.

**c. In the User Name field, type your UNIX or Linux system user name.**

For example, rusty.

This attribute can be used to identify and authenticate users.

**d. In the Email Address field, type your full email address.**

For example, rusty.spanner@indigo-insurance.com.

This attribute can be used to identify and authenticate users.

**FIGURE 4-16** The General Tab for a User Profile

The screenshot shows the 'Secure Global Desktop Administration Console' in a Mozilla Firefox browser window. The console has a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a toolbar with 'Object View', 'Jump To Navigation View', and 'Object History' (set to 'Rusty Spanner'). Below the toolbar is a tabbed interface with tabs for 'General', 'Performance', 'Client Device', 'Printing', 'Security', 'Assigned Applications', 'Passwords', 'Tokens', 'User Sessions', and 'Application Sessions'. The 'General' tab is active, displaying the 'Rusty Spanner - General' form. The form includes a 'Save' button and a 'Reset' button. It shows the user's 'Type' as 'User Profile' and 'Location' as 'User Profiles / organization'. There are expandable sections for 'Designation' and 'Secure Global Desktop Authentication'. The 'Designation' section shows 'Name' as 'Rusty Spanner' and 'Surname' as 'Spanner'. The 'Secure Global Desktop Authentication' section shows 'Login' as 'Enabled', 'Login Name' as 'rusty', and 'Email Address' as 'rusty.spanner@indigo-insurance.com'.

Secure Global Desktop Administration Console - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Object View Jump To Navigation View Object History: Rusty Spanner

General Performance Client Device Printing Security Assigned Applications Passwords Tokens User Sessions Application Sessions

**Rusty Spanner - General** Save Reset

Type: User Profile  
Location: User Profiles / organization

Designation Secure Global Desktop Authentication

Designation

\* Name: Rusty Spanner  
Comment:   
Optional comment field for administrator notes.  
Surname: Spanner  
The surname (family name) of the user. Names can include any characters you want.

Back to top

Secure Global Desktop Authentication

Login: ☒ Enabled ☐ Multiple  
Whether someone may log in using this user profile and whether this user profile will be shared by multiple users in the form of a "guest" account.

Login Name: rusty  
This is typically the UNIX username of the user. This setting can be used to identify and authenticate users.

Email Address: rusty.spanner@indigo-insurance.com  
The email address of the user, in the form 'name@domain'. This setting can be used to identify and authenticate users.

Back to top

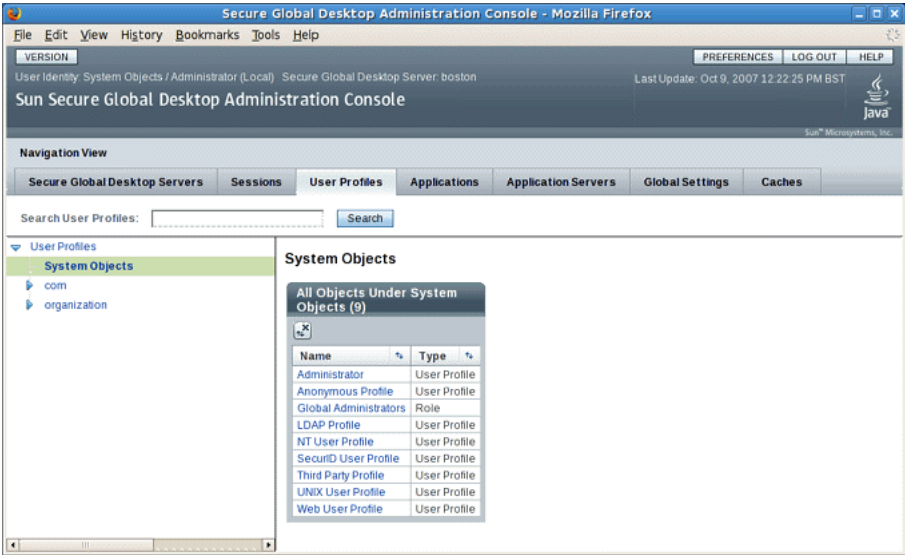
e. Click Save.

## ▼ How to Add an SGD Administrator

1. In the Administration Console, click the User Profiles tab.
2. In the navigation tree, click System Objects.

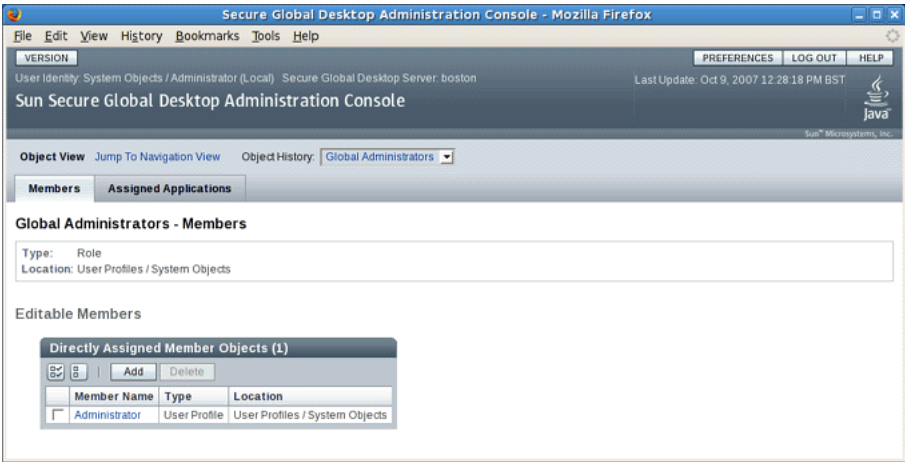
The System Objects table is displayed in the content area, as shown in [FIGURE 4-17](#).

**FIGURE 4-17** The System Objects Table



3. In the System Objects table, click the Global Administrators link.
- The Members tab is displayed in Object View, as shown in [FIGURE 4-18](#).

**FIGURE 4-18** The Members Tab



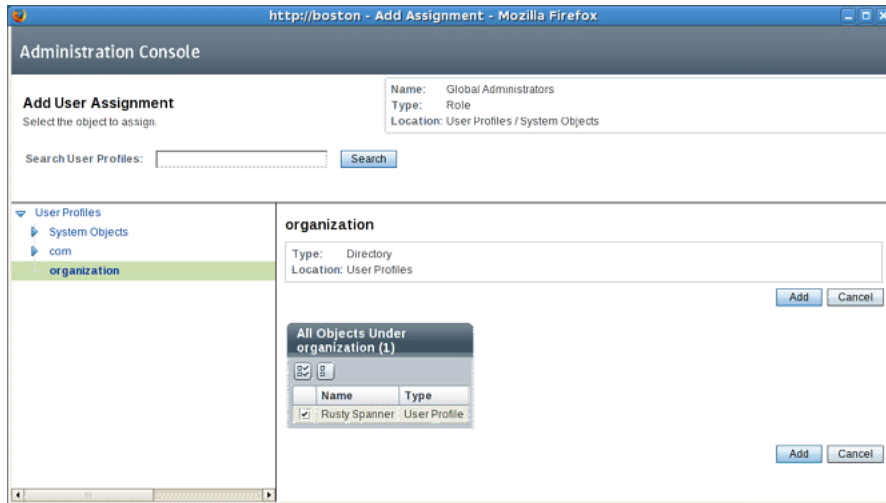
4. In the Editable Members table, click Add.
- The Add User Assignment window is displayed. See [FIGURE 4-19](#).

5. **Locate your user profile.**

Use the Search field to find your user profile, or browse the navigation tree.

6. **Select the check box next to your user profile and click Add.**

**FIGURE 4-19** The Add User Assignment Window



The Members tab is displayed and your user profile is listed in the Editable Members table. See [FIGURE 4-20](#).

**FIGURE 4-20** Updated Members Tab

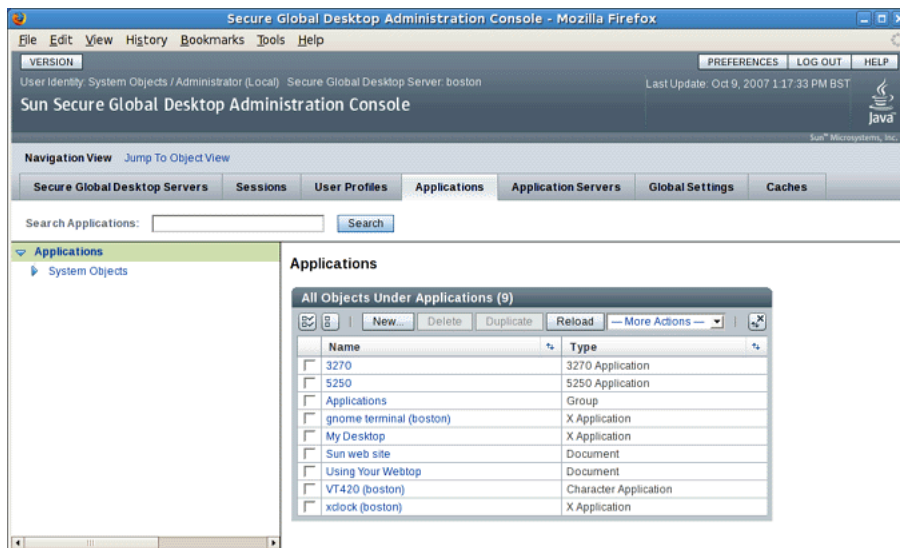


# Adding Applications to Webtops

This section describes how to use the Administration Console to create an application object that can be displayed through SGD, and how to make a link for starting the application appear on a user's webtop.

In the Administration Console, the Applications tab is where you configure the applications that users can run through SGD. See [FIGURE 4-21](#). The Application Servers tab is where you configure the application servers that run the applications. See [FIGURE 4-22](#).

**FIGURE 4-21** The Applications Tab



Application objects are always contained in the Applications organization (o=applications on the command line). Application server objects are always contained in the Application Servers organization (o=appservers on the command line).

You can use Directory (organizational unit) objects to subdivide these organizations. For example, you might want to use a Directory object to contain the applications used by a particular department. You can also arrange applications and application servers into Groups.

In SGD, there are links or relationships between user profiles, applications, and application servers. The Administration Console calls these links assignments. Each relationship is managed from an assignment tab. For example, user profile objects

have an Assigned Applications tab that shows all the application objects that are assigned to the user. These are the applications that display on a user's webtop. Similarly, application objects have a Hosting Application Servers tab that shows the application servers that can run the application.

---

**Tip** – You can configure SGD to use searches of an LDAP directory to assign applications to users. This is called Directory Services Integration (DSI). The *Sun Secure Global Desktop 4.5 Administration Guide* has details of how to configure DSI.

---

## Creating and Assigning an Application Object

Creating and assigning an application object involves the following steps:

1. Create an application server object.

In this step, you specify the name and location of the application server that runs the application.

See [“How to Create an Application Server Object” on page 51](#).

2. Create an application object.

In this step, you specify the command that runs when users start the application and how the application is presented.

See [“How to Create an Application Object” on page 53](#).

3. Assign the application object.

In this step, you assign the application server object to the application object, so that SGD knows where to run the application. Then you assign the application object to an object on the user profiles tab, so that SGD puts a link for the application on a user's webtop.

See [“How to Assign an Application Object” on page 57](#).

Only SGD Administrators can create objects and assign them.

The following procedures describe how to create and assign a Windows application object. The principles are the same for other application types.

On the command line, you can also perform all these steps with the `tarantella` object family of commands.

### ▼ How to Create an Application Server Object

1. In the Administration Console, click the Application Servers tab.

**FIGURE 4-22** The Application Servers Tab



**2. Create the application server object.**

Create the application server object directly in the Application Servers organization, as shown in [FIGURE 4-22](#). You can move it to a different location later if needed.

**a. In the content area, click New.**

The Create a New Object window displays.

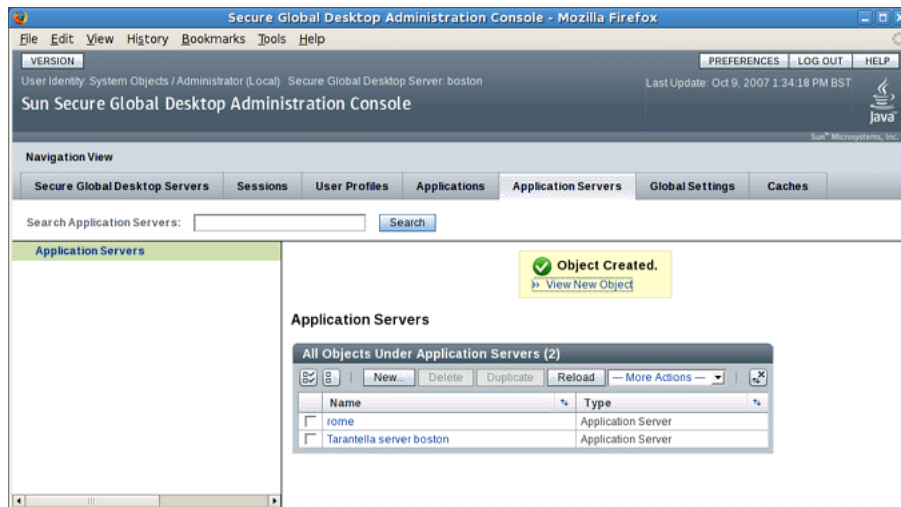
**b. In the Name field, type the name of the application server.**

For example, rome.

**c. Ensure the Application Server option is selected and click Create.**

The Create a New Object window closes and the content area is updated with the new object. See [FIGURE 4-23](#).

**FIGURE 4-23** A Newly-Created Application Server Object



**3. Click the View New Object link.**

The General tab for the application server object is displayed in Object View, as shown in [FIGURE 4-24](#).

**4. Configure the application server object.**

- a. In the Address field, type the fully-qualified Domain Name System (DNS) name of the application server.**

For example, `rome.indigo-insurance.com`.

- b. Ensure that the Application Start check box is selected.**

This tells SGD that the application server is available to run applications.

- c. In the Domain Name field, type the name of the Microsoft Windows domain.**

For example, `rome`.

This attribute is used in the authentication process when users run the application.

**FIGURE 4-24** The General Tab for an Application Server Object

The screenshot shows the 'rome - General' configuration page. At the top, there are tabs for 'General', 'Performance', 'Hosted Applications', 'Application Sessions', and 'Passwords'. The 'General' tab is selected. Below the tabs, there are 'Save' and 'Reset' buttons. The main content area is divided into two sections: 'Designation' and 'Application Authentication'. In the 'Designation' section, there is a 'Name' field with the value 'rome', a 'Comment' field, an 'Address' field with the value 'rome.indigo-insurance.com', and an 'Application Start' checkbox that is checked. In the 'Application Authentication' section, there is a 'Domain Name' field with the value 'rome', a 'Password Cache Usage' section with two radio buttons, and a 'Prompt Locale' field with the value 'en\_us'.

Object View [Jump To Navigation View](#) Object History: [rome](#)

**General** Performance Hosted Applications Application Sessions Passwords

**rome - General** [Save](#) [Reset](#)

Type: Application Server  
Location: Application Servers

[Designation](#) [Application Authentication](#)

**Designation**

\* Name:   
Comment:   
Optional comment field for administrator notes.

Address:  [Test](#)  
The network address of the application server. Using a DNS name rather than an IP address is recommended.

Application Start: ☒ Enabled  
Whether applications can be started on this application server. You can use this setting, for example, to make an application server temporarily unavailable while you carry out maintenance work.

[Back to top](#)

**Application Authentication**

Domain Name:   
The Windows domain to use for the application server authentication process.

Password Cache Usage: ☐ Override Global Setting  
The global setting defines the effective value unless the value is defined here. [See Global Setting](#)

☒ Secure Global Desktop Password Tried  
Whether the password cached during Secure Global Desktop authentication is tried before the password cached during application authentication is tried.

Prompt Locale:   
Locale used when prompting users for authentication. Use the value of a locale defined in file `/opt/aramella/var/serverresources/expect/vars-exp`

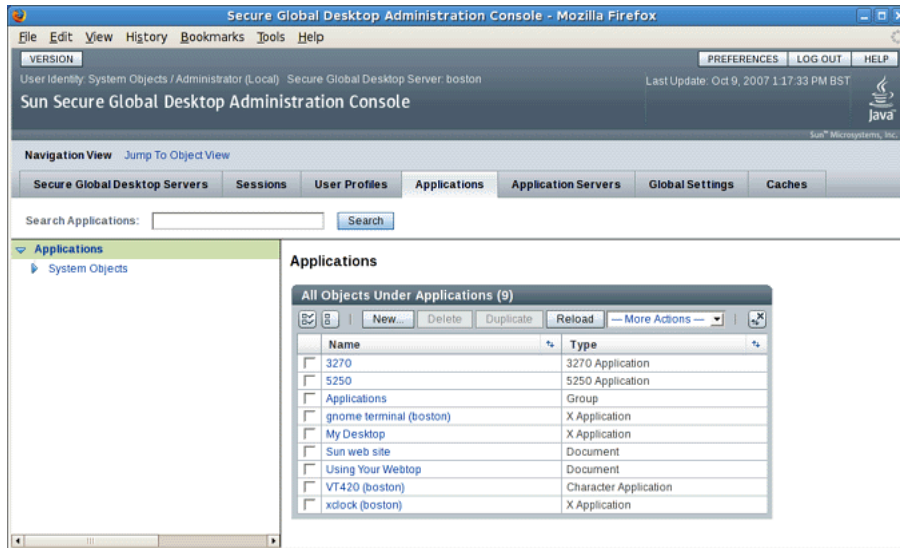
d. Click Save.

## ▼ How to Create an Application Object

The following procedure is an example of how to create a Windows application object.

1. In the Administration Console, click the Applications tab.

**FIGURE 4-25** The Applications Tab



## 2. Create the application object.

Create the application object directly in the Applications organization, as shown in [FIGURE 4-25](#). You can move it to a different location later if needed.

### a. In the content area, click New.

The Create a New Object window displays.

### b. In the Name field, type the name of the application.

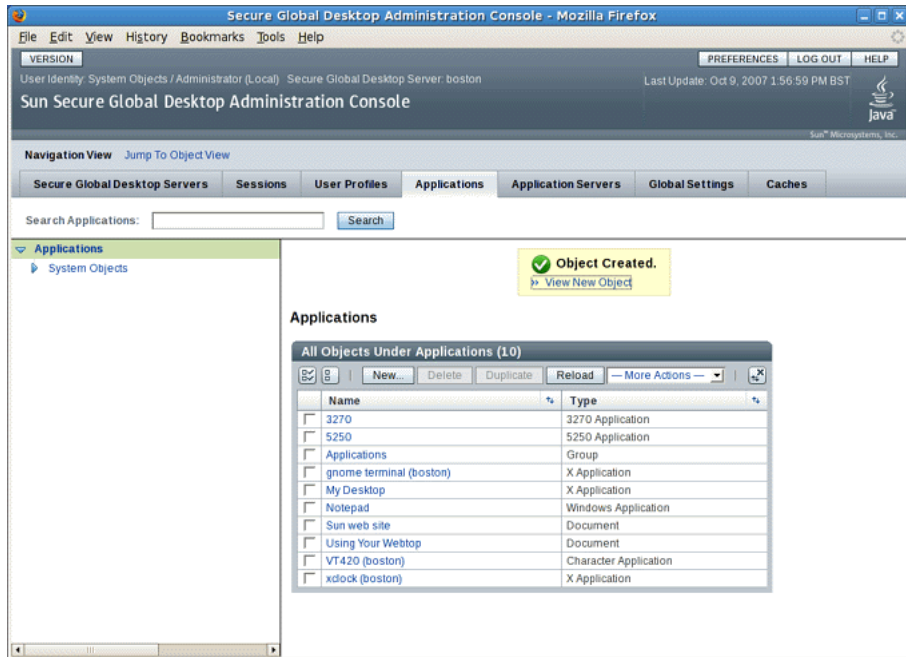
For example, Notepad.

The name you type is used for the application link on the webtop.

### c. Ensure that the Windows Application option is selected and click Create.

The Create a New Object window closes and the content area is updated with the new object, as shown in [FIGURE 4-26](#).

**FIGURE 4-26** A Newly-Created Application Object



**3. Click the View New Object link.**

The General tab for the application object displays in Object View.

**4. Configure the application.**

The configuration settings for a Windows application are described in more detail in the *Sun Secure Global Desktop 4.5 Administration Guide*. For this example, the default settings are sufficient, apart from the following configuration.

**a. Click the Launch tab.**

**b. In the Application Command field, type the application command.**

For Windows desktop sessions, leave this field blank.

To run a particular application, type the full path of the command that runs the application, for example, `C:\Windows\notepad.exe`.

The application must be installed in the same location on all application servers.

**c. Ensure that the Try Running from Application Server check box is selected and that the Microsoft RDP Protocol option is selected.**

**FIGURE 4-27** The Launch Tab

The screenshot shows the 'Launch' tab of the Sun Secure Global Desktop 4.5 configuration interface for the application 'Notepad'. The interface includes a top navigation bar with tabs: Object View, Jump To Navigation View, Object History, and a dropdown menu set to 'Notepad'. Below this is a sub-navigation bar with tabs: General, Launch (selected), Presentation, Performance, Client Device, Hosting Application Servers, Assigned User Profiles, and Application Sessions. The main content area is titled 'Notepad - Launch' and contains several configuration fields: 'Type' (Windows Application), 'Location' (Applications), 'Application Command' (C:\Windows\notepad.exe), 'Arguments for Command' (empty text box), 'Windows Protocol' (radio buttons for Try Running from Client First, Try Running from Application Server (selected), Microsoft RDP Protocol, and Citrix ICA Protocol), 'Arguments for Protocol' (empty text box), 'Domain Name' (empty text box), and 'Login Script' (windows.exp). There are 'Save' and 'Reset' buttons in the top right corner of the configuration area.

**d. Click Save.**

**5. Click the Presentation tab.**

**a. Configure the Window type.**

For a Windows desktop session, select the Kiosk setting from the list.

For an individual application, select the Independent Window setting from the list. You can use the Window Size options to specify the size of the window.

**FIGURE 4-28** The Presentation Tab

**Object View** [Jump To Navigation View](#) Object History: [Notepad](#)

**General** **Launch** **Presentation** **Performance** **Client Device** **Hosting Application Servers** **Assigned User Profiles** **Application Sessions**

**Notepad - Presentation** [Save](#) [Reset](#)

Type: Windows Application  
Location: Applications

Window Type: [Independent Window](#) is recommended for applications with many top-level resizable windows. Independent Window is recommended for Windows  
[Seamless Window](#) is recommended for full-screen desktop sessions. Seamless Window is not recommended for full-screen desktop sessions: use a kiosk or  
[Kiosk](#)

Window Manager:

Any Window Manager to use for the application. You can also use this to name any other applications to run alongside the main application. You can name as many applications as you want.

Window Size: ☐ Client's Maximum Size Check the box to ensure the application fills the user's screen when it starts. Clear the box to size the application according to the object's Width and Height settings  
☐ Scale to Fit Window If this setting is checked, the application is always scaled to fit the window in which it is displayed. If you re-size the window, Secure Global Desktop scales the application to fit the new window size and scroll bars will never display.

Width:  pixels The minimum width is 10 pixels, the maximum 65535 pixels.  
Height:  pixels The minimum height is 10 pixels, the maximum 65535 pixels.

Color Depth: [16-bit - Thousands of colors](#) The greater the number of colors, the more memory is required on the Secure Global Desktop server and on the client device, and the more network bandwidth is used between them.

[Save](#) [Reset](#)

**b. Click Save.**

## ▼ How to Assign an Application Object

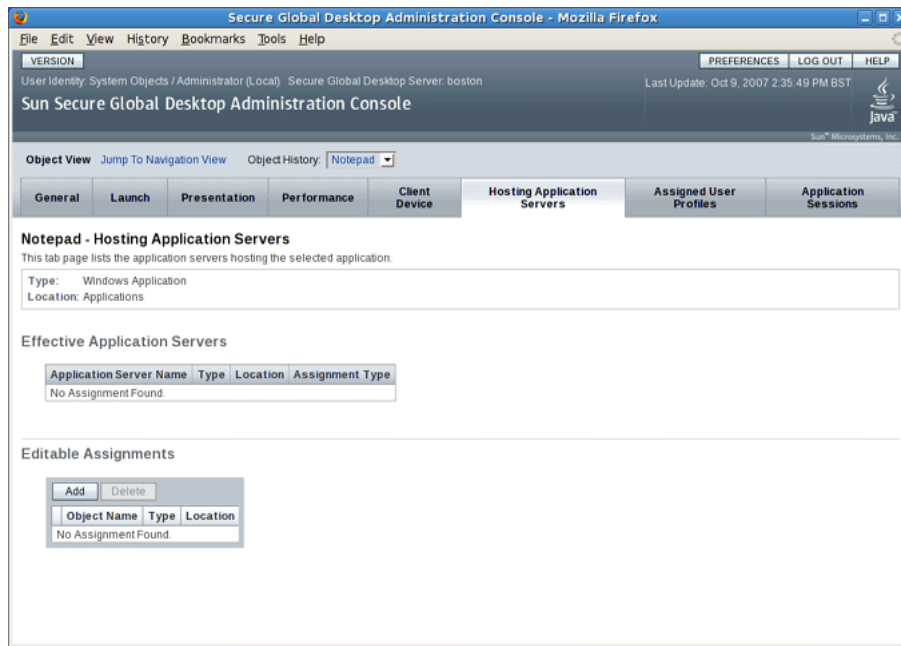
- 1. In the Administration Console, click the Applications tab and select the application object.**

The General tab is displayed in Object View.

- 2. Specify the application servers that can run the application.**

**a. Click the Hosting Application Servers tab. See [FIGURE 4-29](#).**

**FIGURE 4-29** The Hosting Application Servers Tab



**b. In the Editable Assignments table, click Add.**

The Add Application Server Assignment window displays. See [FIGURE 4-30](#).

**c. Locate the application server.**

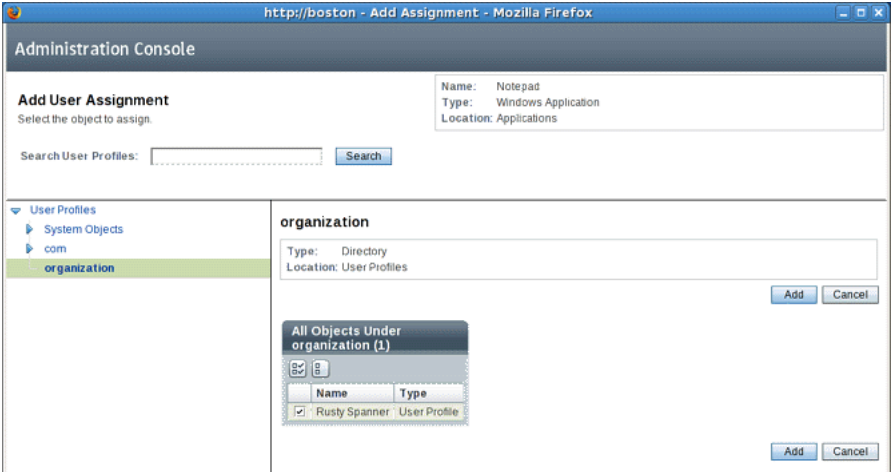
Use the Search field to find the application server object, or browse the navigation tree.

**d. Select the check box next to the application server object and click Add**

If you select more than one application server object, SGD load balances between application servers.

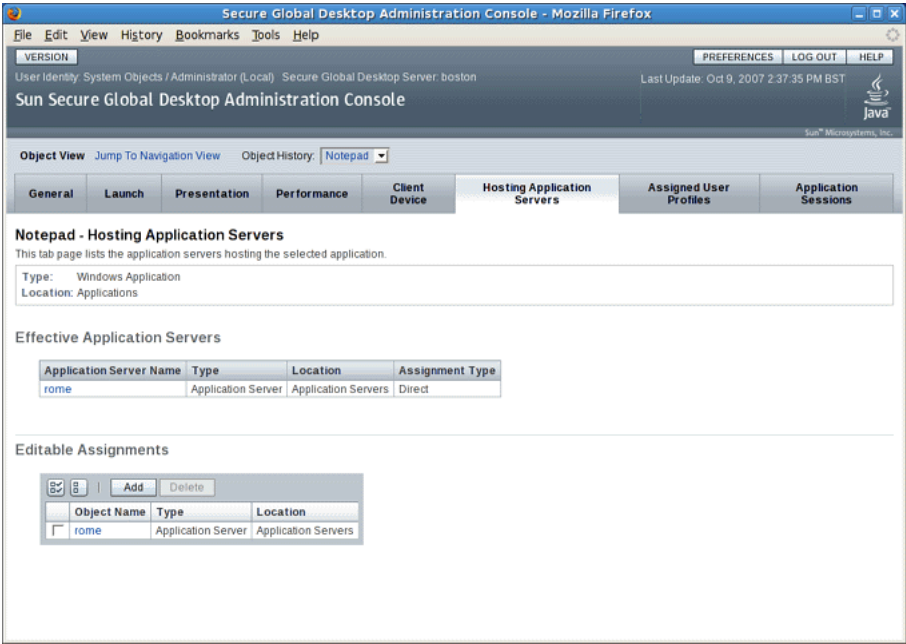
If you select a group object containing application server objects, you select all the application server objects in that group.

**FIGURE 4-30** The Add Application Server Assignment Window



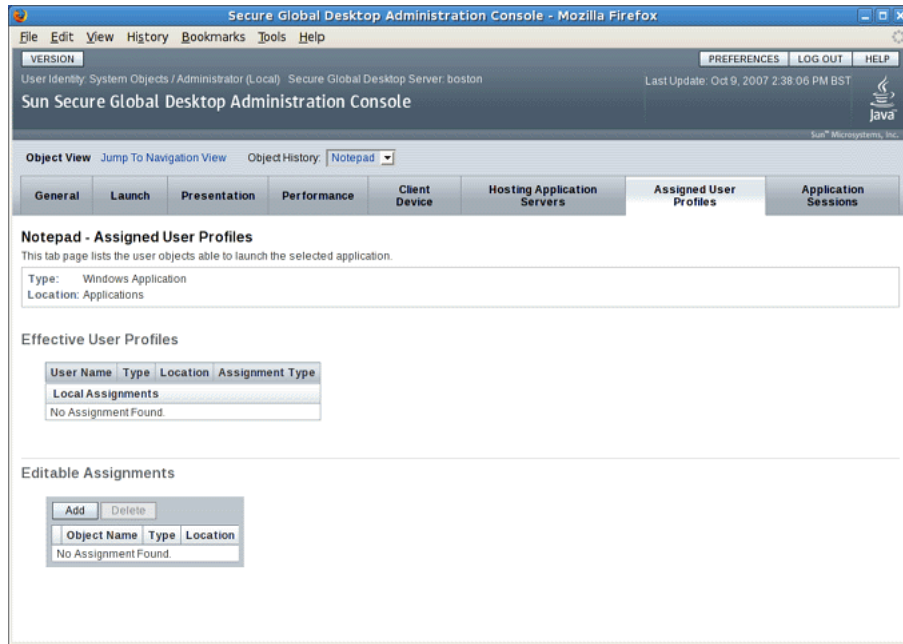
The Effective Application Servers table is updated with the selected application server object, as shown in [FIGURE 4-31](#).

**FIGURE 4-31** Updated Hosting Application Servers Tab



3. Specify the users that see the application on their webtop.
  - a. Click the Assigned User Profiles Tab. See [FIGURE 4-32](#).

**FIGURE 4-32** The Assigned User Profiles tab



**b. In the Editable Assignments table, click Add.**

The Add User Assignment window displays, as shown in [FIGURE 4-33](#).

**c. Locate the user profile.**

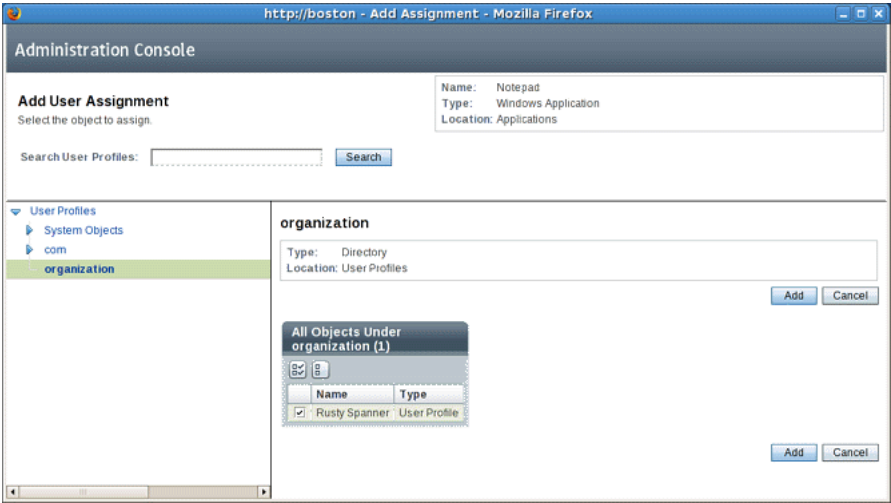
Use the Search field to find the user profile, or browse the navigation tree.

You can assign an application object to a user profile or directory object.

If you assign an application object to a directory object, all the user profiles contained in that directory object automatically receive the application. This is called inheritance. Assigning an application object to directory objects is more efficient.

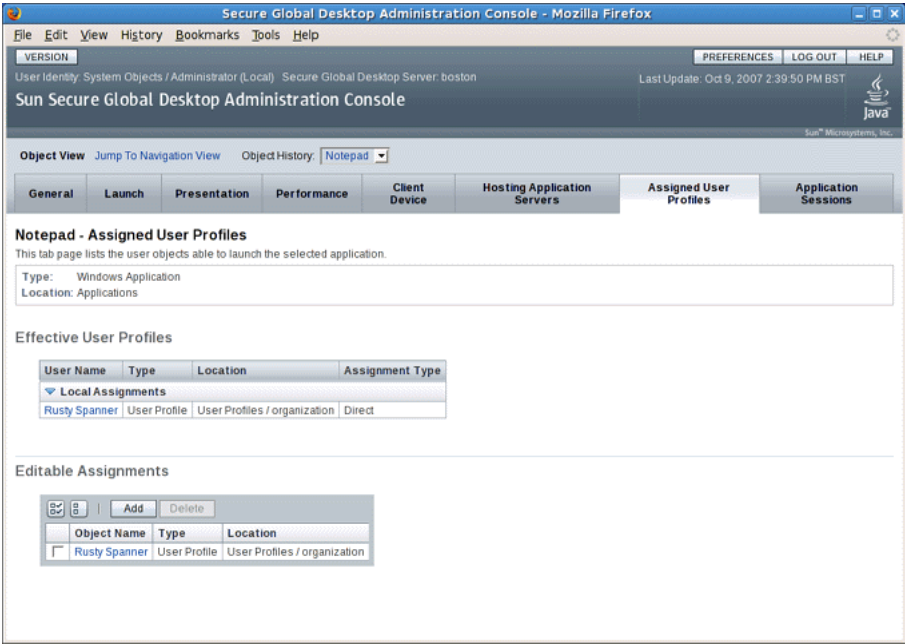
**d. Select the check box next to your user profile and click Add.**

FIGURE 4-33 The Add User Assignment Window



The Effective User Profiles table is updated with the selected users. See [FIGURE 4-34](#).

FIGURE 4-34 Updated Assigned User Profiles Tab



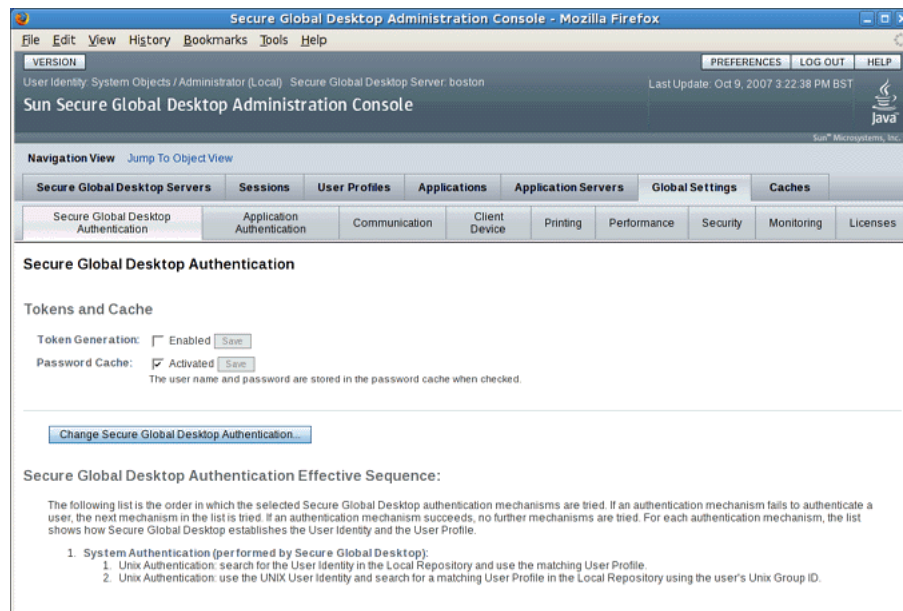
#### 4. Check that the application appears on your webtop.

You might have to log out and log in using your UNIX or Linux system user name and password to see the application on your webtop.

## Managing SGD

In the Administration Console, the Global Settings tab is where you configure the settings that apply to SGD as a whole. See [FIGURE 4-35](#).

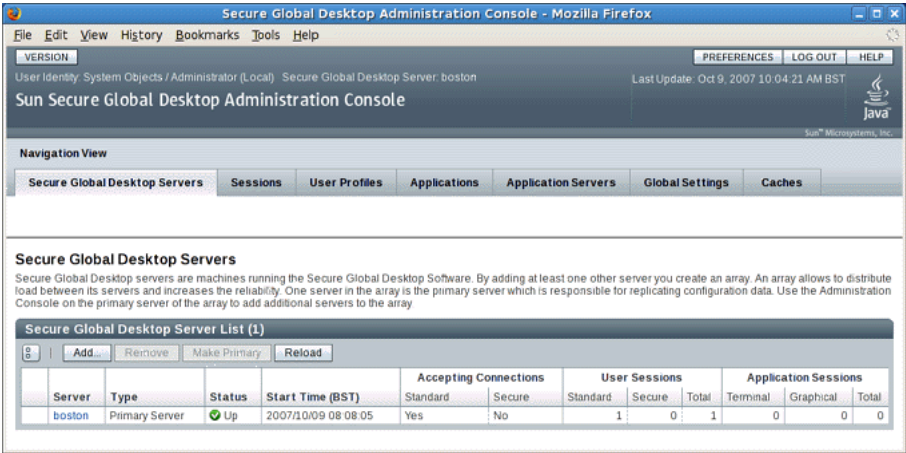
**FIGURE 4-35** The Global Settings Tab



The Global Settings tab contains other tabs for configuring and managing SGD. For example, the Secure Global Desktop Authentication tab is where you configure how users authenticate to SGD.

In the Administration Console, the Secure Global Desktop Servers tab is where you manage individual SGD servers. See [FIGURE 4-36](#).

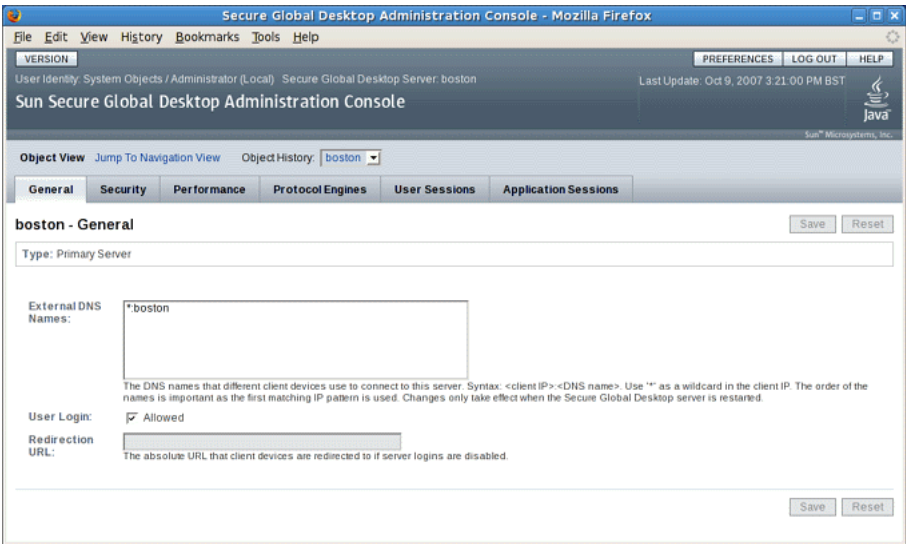
FIGURE 4-36 The Secure Global Desktop Servers Tab



The Secure Global Desktop Servers tab shows you the status of an SGD server, whether it is running, how many user sessions there are, and how many application sessions the server is hosting.

When you click on the name of an SGD server in the Secure Global Desktop Servers List table, the Administration Console displays further tabs in Object View. You use these tabs to configure and manage the selected SGD server. See [FIGURE 4-37](#).

FIGURE 4-37 The General Tab for an SGD Server



On the command line, you use the `tarantella config` command to configure global settings and SGD servers. The *Sun Secure Global Desktop 4.5 Administration Guide* has details of all the command-line arguments.

## Arrays

The Secure Global Desktop Servers tab enables you to group SGD servers together to form an *array*. An array is a collection of SGD servers that share configuration information.

An array contains the following:

- **One primary server** – This server is the authoritative source for global SGD information, and maintains the definitive copy of the organizational hierarchy
- **One or more secondary servers** – The primary server replicates information to these servers

A single, *standalone* server is considered to be the primary server in an array with no secondary servers.

SGD servers in an array might run different operating systems. However, all the array members must run the same version of SGD.

While you are evaluating SGD you are limited to an array containing a maximum of two SGD servers. Once you install a license key, this restriction is removed.

Arrays have the following benefits:

- User sessions and application sessions are load-balanced across the array. To scale more users, simply add more SGD servers to the array.
- With more than one server, there is no single point of failure. You can decommission a server temporarily with the minimum of disruption to your users.
- Configuration information, including all the objects in your organizational hierarchy, is replicated to all array members. All array members have access to all information.

Users see the same webtop and can resume applications no matter which SGD server they log in to.

You add an SGD server to an array by clicking Add in the Secure Global Desktop Servers List table.

# Monitoring Users

You can keep track of what your users are doing by monitoring the user sessions and application sessions in progress. User sessions and application sessions are always associated with a user identity and a user profile. The user identity is the unique authenticated identity of the user. The user profile is the SGD user profile object that contains the user's settings.

## User Sessions

A user session begins when a user logs in to SGD and ends when a user logs out. User sessions are hosted by the SGD server the user logs in to. User sessions can be standard sessions or secure sessions. Secure sessions are only available when SGD security services are enabled.

If a user logs in and they already have a user session, the user session is transferred to the new SGD server and the old session ends. This is sometimes called session grabbing, or session moving.

In the Administration Console, you can list user sessions as follows:

- The Sessions tab, in Navigation View, shows all the user sessions that are running on all SGD servers in the array.
- The User Sessions tab for an SGD server shows all the user sessions that are hosted by that server.
- The User Sessions tab for a user profile shows all the user sessions associated with the user profile.

On the Sessions tab and the User Sessions tabs, you can select and end user sessions. On the User Sessions tabs, you can view further details about the user session, for example the information the SGD Client detects about the client device.

On the command line, you use the `tarantella webtopsession` command to list and end user sessions.

## Application Sessions

An application session begins when a user starts an application and ends when the application exits. Each application session corresponds to an application currently running through SGD. Application sessions can be running or suspended.

An application session can be hosted by any SGD server in the array. This might not be the same SGD server that the user logged in to.

In the Administration Console you can list application sessions as follows:

- The Application Sessions tab for an SGD server shows all the application sessions that are hosted by that server.
- The Application Sessions tab for a user profile shows all the application sessions associated with the user profile.
- The Application Sessions tab for an application server shows all the applications that are running on that application server.

On the Applications Sessions tabs, you can view further details about an application session. You can also end and *shadow* application sessions. With shadowing, you and the user see and interact with the application at the same time.

---

**Note** – You can only shadow Windows applications and X applications, and the application sessions must not be suspended.

---

See [“How to Shadow a User’s Application Session” on page 66](#) for details of how to shadow an application session.

On the command line, you use the `tarantella emulatorsession` command to list, end, and shadow application sessions.

## ▼ How to Shadow a User’s Application Session

If a user is having difficulty with an application, you can use the Administration Console to find the user’s application session and then shadow it.

### 1. Find the user’s application session.

In the Administration Console, do one of the following:

- Go to the Application Sessions tab for the user profile object.  
This tab lists the application sessions for a user.
- Go to the Application Sessions tab for the application object.  
This tab lists the users who are currently running the application.

### 2. Select the application session in the Application Sessions List table.

### 3. Start shadowing of the application session.

Click the Shadow button.

The user sees a dialog box, asking whether to allow you to shadow the session. If the user agrees, a new window appears on your screen, showing the running application. Both you and the user can control the mouse pointer and use the application.

#### 4. After fixing the user's problem, end shadowing of the application session.

Close the shadowing window, but do not close the application.

The user sees a dialog box, saying that nobody is currently shadowing the session.

---

## Controlling SGD

To control SGD from the command line, use the `tarantella start`, `tarantella stop`, and `tarantella restart` commands.

You control an SGD server *and* the SGD web server with the following commands:

- `tarantella start` – Starts the SGD web server and the SGD server
- `tarantella stop` – Stops the SGD web server and the SGD server
- `tarantella restart` – Stops and then restarts the SGD web server and the SGD server

Subcommands for the `tarantella start`, `tarantella stop`, and `tarantella restart` commands enable you to control individual components of SGD, as follows:

- The `sgd` subcommand controls the SGD server. The following example starts SGD services on a host, including printing services.

```
# tarantella start sgd
```

- The `webserver` subcommand controls the SGD web server. The following example stops and then restarts the SGD web server.

```
# tarantella restart webserver
```

See the *Sun Secure Global Desktop 4.5 Administration Guide* for more information about the available subcommands and options for the `tarantella stop`, `tarantella start`, and `tarantella restart` commands.

## Controlling the SGD Enhancement Module

This section describes how you control the SGD Enhancement Module.

## Controlling the SGD Enhancement Module for Microsoft Windows

When you install the SGD Enhancement Module for Microsoft Windows, the load balancing service starts immediately. The load balancing service also starts automatically whenever the Windows host is rebooted.

### ▼ How to Manually Control the Load Balancing Service

Use the following procedure to manually stop and start the load balancing service on a Windows host.

1. **Log in to the Windows host as a user with administrative privileges.**
2. **In the Windows Control Panel, click Administrative Tools.**
3. **Click Computer Management.**
4. **In the tree, expand Services and Applications.**
5. **Click Services.**
6. **Double-click the Tarantella Load Balancing Service.**
7. **Click Stop or Start to stop or start the service.**

## Controlling the SGD Enhancement Module for UNIX and Linux Platforms

When you install the SGD Enhancement Module for UNIX and Linux Platforms, the load balancing and UNIX audio processes start immediately. The client drive mapping processes have to be started manually because extra configuration is required.

Whenever the host is rebooted, all the Enhancement Module processes are started automatically.

On UNIX and Linux platforms, you can control the Enhancement Module processes manually with the `tem` command. The `tem` command is a script installed in the `install-dir/bin` directory. By default, `install-dir` is `/opt/tta_tem`. As this script is not on the standard `PATH`, you must use the full path each time you run the command, or change to `/opt/tta_tem/bin` before running the command. Alternatively, do the following:

- Add `/opt/tta_tem/bin` to the `PATH`, for example:

```
PATH=$PATH:/opt/tta_tem/bin; export PATH
```

- Create an alias, for example:

```
alias em=/opt/tta_tem/bin/tem
```

You control the Enhancement Module processes manually by running the following commands as superuser (root):

- `tem start` – Starts the load balancing processes
- `tem stop` – Stops the load balancing processes
- `tem startcdm` – Starts the CDM processes
- `tem stopcdm` – Stops the CDM processes
- `tem startaudio` – Starts the UNIX platform audio processes
- `tem stopaudio` – Stops the UNIX platform audio processes

Use the `tem status` command to show the status of the various modules in the Enhancement Module.

---

## SGD Network Architecture

SGD is built around a three-tier network architecture model, consisting of the following tiers:

- Client devices
- SGD servers
- Application servers

Different tiers can reside on the same host. For example, a single UNIX platform host can act as both an SGD server and an application server, but the tiers remain logically independent.

### Client Devices

The first tier contains *client devices*. A client device is a piece of hardware that can communicate with SGD using a browser and the SGD Client.

The browser communicates with the SGD web server on the second tier and displays the webtop to users.

The SGD Client communicates with SGD servers on the second tier and displays the applications that users run.

The Adaptive Internet Protocol (AIP) ensures optimal network usage between the first and second tiers.

## SGD Servers

The second tier contains *SGD servers*, which act as a gateway between the first and third tiers. This tier might contain a single SGD server, or many SGD servers configured to form an array.

An SGD server is responsible for the following:

- Authenticating users when they log in to SGD
- Negotiating with application servers to authenticate users when they run applications, prompting users for passwords when necessary
- Causing the SGD Client to display applications
- Keeping track of running applications even after users have logged out, so that they can resume them later

## Application Servers

The third tier contains *application servers* that run users' applications.

When a user clicks a link on their webtop, SGD starts the application on an appropriate application server. Output from the application is redirected by the SGD server from the application server to the client device.

When you tell SGD about an application, you include information about all the application servers that can run the application. SGD load balances between the application servers.

---

## Next Steps

By default, SGD installs in a 30-day evaluation mode. During the evaluation period, the following restrictions apply:

- The size of an array is limited to two SGD servers.
- The number of users that can log in or have running applications is limited to five.

After 30 days, the SGD server no longer permits users to log in.

To continue using SGD, you must add a license key. You can add license keys in the following places:

- On the Licenses tab in the Administration Console

- On the command line:

```
# tarantella license add license-key
```

## What You Need to Tell Users

The following information is essential to help people use SGD:

- How to log in to SGD.

Users need to know the login URL. Use `http://server.example.com/sgd`, where *server.example.com* is the name of an SGD server.

Users need to know what user name and password to type to log in to SGD.

SGD supports several mechanisms for authenticating users. The user names and passwords depend on the enabled authentication mechanisms. By default, users can log in with their UNIX or Linux system user name and password.

If your organization prefers not to use Java technology, users need to be shown how to download and install the SGD Client manually. See [“Installing the SGD Client Manually” on page 18](#) for details.

- How to run applications.

Users need to know how to start and stop applications.

The applications users can access through SGD might run on many different application servers. When a user clicks a link to start an application, SGD might prompt them for a user name and password for the application server. Users need to know what user names and passwords to use.

- Where to get help.

All users have a link to the *Sun Secure Global Desktop 4.5 User Guide* on their webtop. Click Help.

## Where to Get More Help

On the webtop, click Help to display the *Sun Secure Global Desktop 4.5 Administration Guide*. This is the online documentation for configuring and running SGD. Online help is also available in the Administration Console.

Documentation in Hypertext Markup Language (HTML) and Portable Document Format (PDF) formats is also available from the following locations:

- `http://server.example.com`, where *server.example.com* is the name of an SGD server
- (<http://docs.sun.com/app/docs/coll/1706.4>)

You can also discuss technical issues at the SGD forum on Sun Developer Network (<http://forum.java.sun.com/forum.jspa?forumID=815>).

## Removing SGD

---

This chapter describes how you remove Sun Secure Global Desktop (SGD).

---

## Removing SGD

To remove SGD, you remove the components installed on hosts, on application servers, and on client devices.

### ▼ How to Remove SGD

1. Log in as superuser (root) on the SGD host.
2. Remove SGD.

```
# tarantella uninstall --purge
```



---

**Caution** – The `tarantella uninstall` command is the only supported method for removing SGD. This command stops all SGD processes before removing the software. Do not use the `pkgmgr` or `rpm` commands directly to remove SGD.

---

### ▼ How to Remove the SGD Enhancement Module for Microsoft Windows

1. Log in to the Windows host as a user with administrator privileges.

2. In the Windows Control Panel, select Add or Remove Programs.
3. Select Secure Global Desktop Enhancement Module for Windows.
4. Click Remove.

## ▼ How to Remove the SGD Enhancement Module for UNIX<sup>®</sup> and Linux Platforms

1. Log in as superuser (root) on the application server.
2. Remove the Enhancement Module.

The following commands stop all Enhancement Module processes before removing the software.

On Solaris<sup>™</sup> Operating System (Solaris OS) platforms:

```
# pkgrm tem
```

On Linux platforms:

```
# rpm -e tem
```

---

**Note** – The Enhancement Module installation directory, and some configuration files in this directory, are not removed. The default installation directory for the Enhancement Module is /opt/tta\_tem.

---

## ▼ How to Remove the SGD Client on Microsoft Windows Platforms (Manual Installation)

Follow these instructions only if the SGD Client was installed manually.

1. In the Windows Control Panel, select Add or Remove Programs.
2. Select Sun Secure Global Desktop Client.
3. Click Remove.

## ▼ How to Remove the SGD Client on Microsoft Windows Platforms (Automatic Installation)

Follow these instruction only if the SGD Client was installed automatically.

- **Remove the SGD Client program.**

Delete the SGD Client program from the user's Home folder. Typically this is the `C:\Documents and Settings\username\Local Settings\Temp\tcc\version` folder.

The SGD Client program is `tcc.exe`.

## ▼ How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms

- **Remove the SGD Client program.**

Delete the SGD Client program from wherever it is installed. Typically this is either the `$HOME/.tarantella/tcc/version` directory or the `$HOME/bin` directory.

The SGD Client program is `ttatcc`.

